



# WIPO CASE

Dr. Juneho Jang  
Senior Regional Manger

# Outline

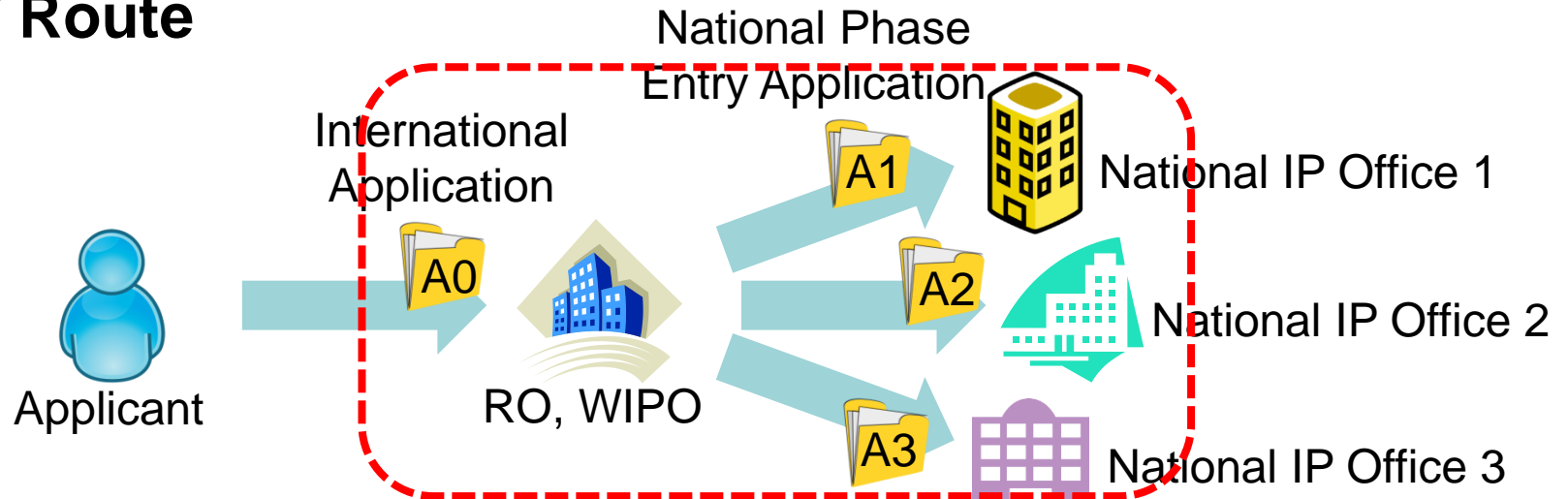
- **Background**
- **WIPO CASE Service**
- **Functions of WIPO CASE**
- **Future Development**

# Outline

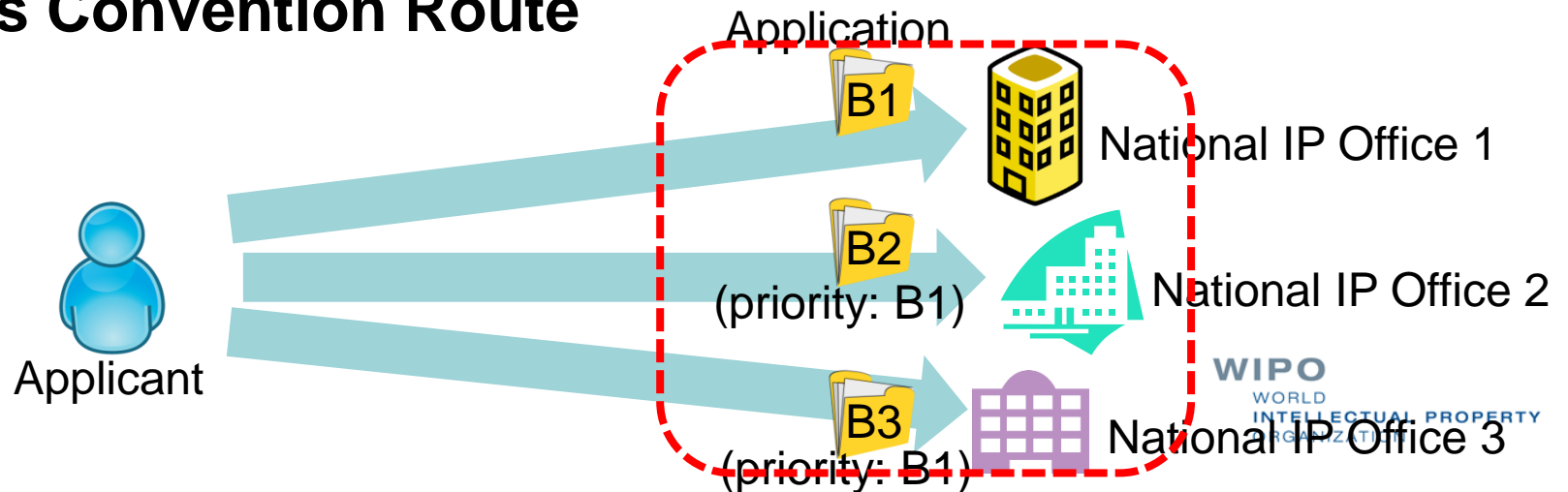
- **Background**
- WIPO CASE Service
- Functions of WIPO CASE
- Future Development

# Patent Family

## ■ PCT Route

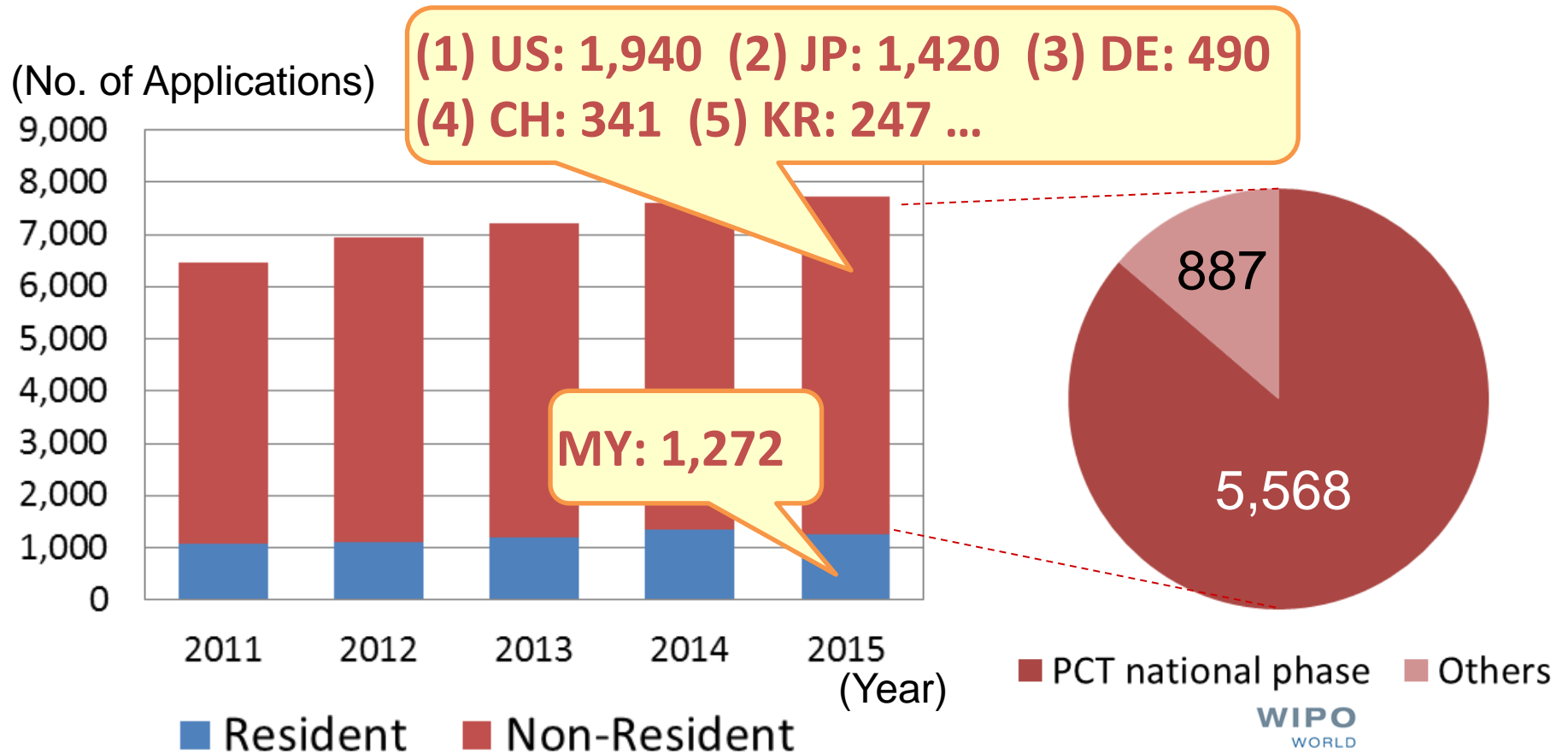


## ■ Paris Convention Route



# Patent Family

## Patent Applications in Malaysia



# Utilization of Dossier Information

## ■ Examination Process



Understanding



Search



Examination

(judgement, communication)

- Understand the application better

Dossier Information  
(search/exam report,  
applicant's opinion, etc.)

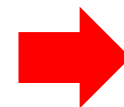


- Reduce the time for  
search/examination

- Carry out further  
search/examination in  
consideration of existing  
information



How to get dossier information?



**WIPO CASE**

OPERTY

WIPO

# What is “WIPO CASE”?

## WIPO CASE (Centralized Access to Search and Examination)

A worldwide online platform to share information on patent search and examination results among participating national IP offices.

### Patent Family Search

Home IP Services WIPO CASE Search Preferences Users Notifications Notifications Data Coverage Statistics User Guide About

WIPO CASE

Application Number  Extended Simple e.g.: ( MYPI20000041, MYPI20000344 ) Compare Maximize Close all tabs

MY2012004612

Time Line Tabular View Family Citations Discussion View Application Subscribe Family Subscribe Update Indicators

Timeline view showing patent family members:

- GB1006460.8 (2009)
- PCT/GB2011/050740 (2011)
- AU2011244808 (2011)
- MY2012004612 (2012)
- US13/640,437 (2012)

### Dossier Information Access

Home IP Services WIPO CASE Search Preferences Users Notifications Notifications Data Coverage Statistics User Guide About

WIPO CASE

Application Number  Extended Simple e.g.: ( MYPI20000041, MYPI20000344 ) Compare Maximize Close all tabs

MY2012004612

AU2011244808

Document List

Document Name	Date	Pages/Size	Actions
CORRO OUT	2014-11-16	0.18 MB	Download Print Share
DESCRIPTION	2014-11-17	0.51 MB	Download Print Share
CLAIM	2014-11-17	0.05 MB	Download Print Share
AMENDMENT	2014-10-10		Download Print Share
AMENDMENT	2014-10-10	0.81 MB	Download Print Share
EXAM CORRO	2013-05-16	0.35 MB	Download Print Share
ABSTRACT	2012-10-18	0.08 MB	Download Print Share
DRAWING	2012-10-18	0.06 MB	Download Print Share
DRAWING	2012-10-18	0.06 MB	Download Print Share
DESCRIPTION	2012-10-18	0.49 MB	Download Print Share
CLAIM	2012-10-18	0.04 MB	Download Print Share
ABSTRACT	2012-10-18	0.08 MB	Download Print Share

Document: EXAM CORRO (2013-05-16)

Australian Government  
IP Australia

Address: Davies Colson Cave  
Level 15  
1 Nicholson Street  
MELBOURNE VIC 3000  
Australia

Date of issue: 16 May 2013

**Modified Patent Examination Report No. 1**

Application Details

Patent Application No.: 201244808  
Applicant(s): Techstep France  
Your reference: 351527ZPSH  
Earliest Priority Date: 19 April 2010  
Examination Request Date: 24 January 2013

Your application has been examined under Section 48 of the Patents Act 1990. I consider that the application does not meet the requirements of the Act for the reasons indicated below.

Actions you can take

You have 21 months from the date of this report to overcome all my objection(s) otherwise your application will lapse.

You will need to pay a monthly fee for any response you file after 12 months from the date of the first report.

You will also need to pay any annual continuation fees that apply. Information about fees may be obtained by phoning 1300 651 610 or by visiting [www.ipaustralia.gov.au](http://www.ipaustralia.gov.au).

Bibliographic Data  
Citation Data

View 1 - 12 of 12

# What is “WIPO CASE”?

Examine

Examine

Improve  
**Efficiency** and **Quality**

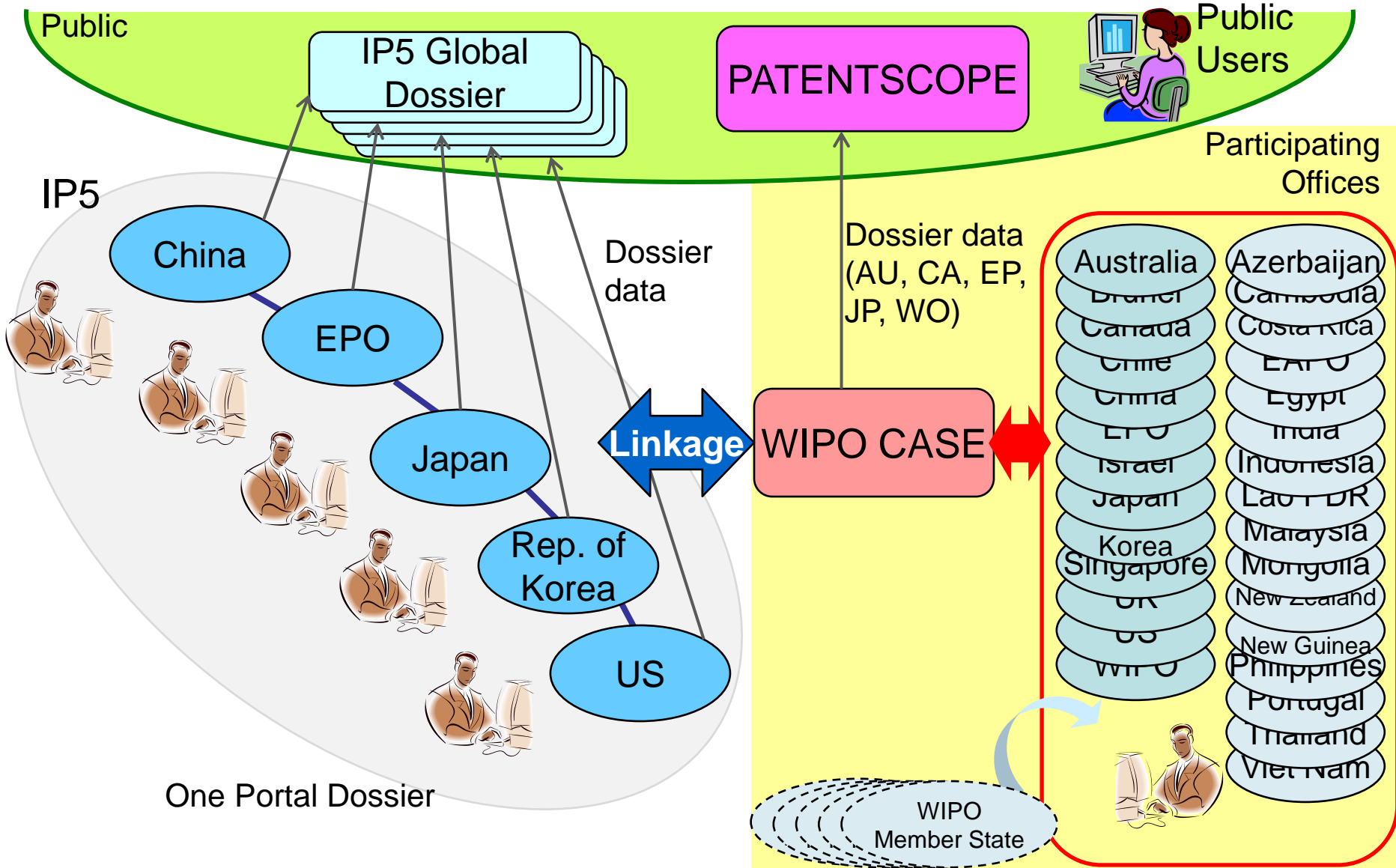
File

Applicant

IP Office B



# WIPO CASE Network



# WIPO CASE Evolution

- **March 2011** – Became operational for Vancouver Group Offices (AU, CA and GB)
- **July 2012** – Access to AU application data and documents through web services
- **March 2013** – New Framework Provisions open up the system for membership for all IP offices of WIPO member states.
- **September 2013** – Access to PCT application data and documents
- **April 2014** – Linkage between One Portal Dossier and WIPO CASE. Japan and 5 other offices participate in the pilot project.
- **March 2015** – New web portal and forum functionality
- **June 2015** – New Terms and Conditions simplify the governance structure and allow for public access.
- **August 2016** – All IP5 offices linked through CASE – OPD linkage
- **January 2017** – Dossier content can be accessed via PATENTSCOPE

# WIPO CASE Membership

## ■ Providing Office

Share its dossier information with other participating offices

## ■ Accessing Office

Permitted to access WIPO CASE to retrieve dossier information from Providing Offices



# WIPO CASE Membership

## – Providing Offices

Offices	Providing Office	Accessing Office	Notes
AU (Australia)	Yes	Yes	Provided to the public
BN (Brunei Darussalam)	Yes	Yes	Not yet operational
CA (Canada)	Yes	Yes	Provided to the public
CL (Chile)	Yes	Yes	Not yet operational
CN (China)	Yes	Yes	
EP (EPO)	Yes	Yes	Provided to the public
GB (United Kingdom)	Yes	Yes	
IL (Israel)	Yes	Yes	
JP (Japan)	Yes	Yes	Provided to the public
KR (Republic of Korea)	Yes	Yes	
SG (Singapore)	Yes	Yes	Not yet operational
US (United States of America)	Yes	Yes	
WO (WIPO IB (PCT))	Yes	No	Provided to the public

# WIPO CASE Membership

## - Accessing-only Offices

Offices	Providing Office	Accessing Office
AZ (Azerbaijan)	No	Yes
CR (Costa Rica)	No	Yes
EA (EAPO)	No	Yes
EG (Egypt)	No	Yes
GE (Georgia)	No	Yes
ID (Indonesia)	No	Yes
IN (India)	No	Yes
KH (Cambodia)	No	Yes
LA (Lao PDR)	No	Yes
MN (Mongolia)	No	Yes

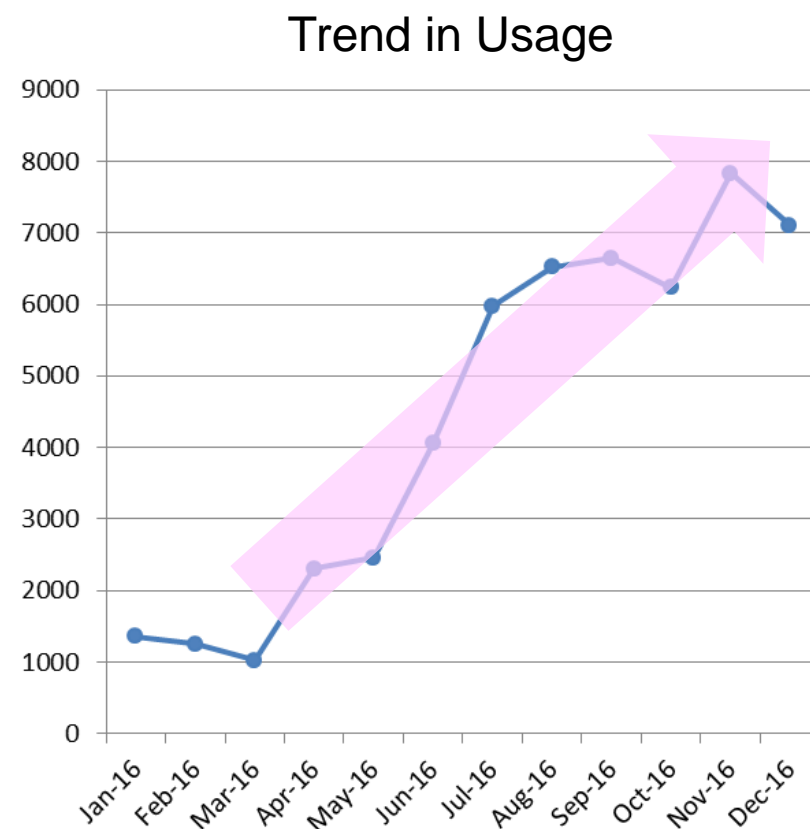
Offices	Providing Office	Accessing Office
MY (Malaysia)	No	Yes
NZ (New Zealand)	No	Yes
PG (Papua New Guinea)	No	Yes
PH (Philippines)	No	Yes
PT (Portugal)	No	Yes
TH (Thailand)	No	Yes
VN (Viet Nam)	No	Yes

(as of June, 2017)

# Usage of WIPO CASE

- Period: January, 2016 – December, 2016
- Total: 107,735 (based on Counts of Accessed Documents)
- Statistics:

Accessing Office	Usage	
	Count	Percentage of Total
CN	18,035	34.2%
JP	12,047	22.8%
KR	8,211	15.6%
EP	7,097	13.5%
GB	2,032	3.9%
AU	1,688	3.2%
CA	1,487	2.8%
PH	1,079	2.0%
ID	520	1.0%
NZ	156	0.3%
TH	154	0.3%
IL	129	0.2%



# Outline

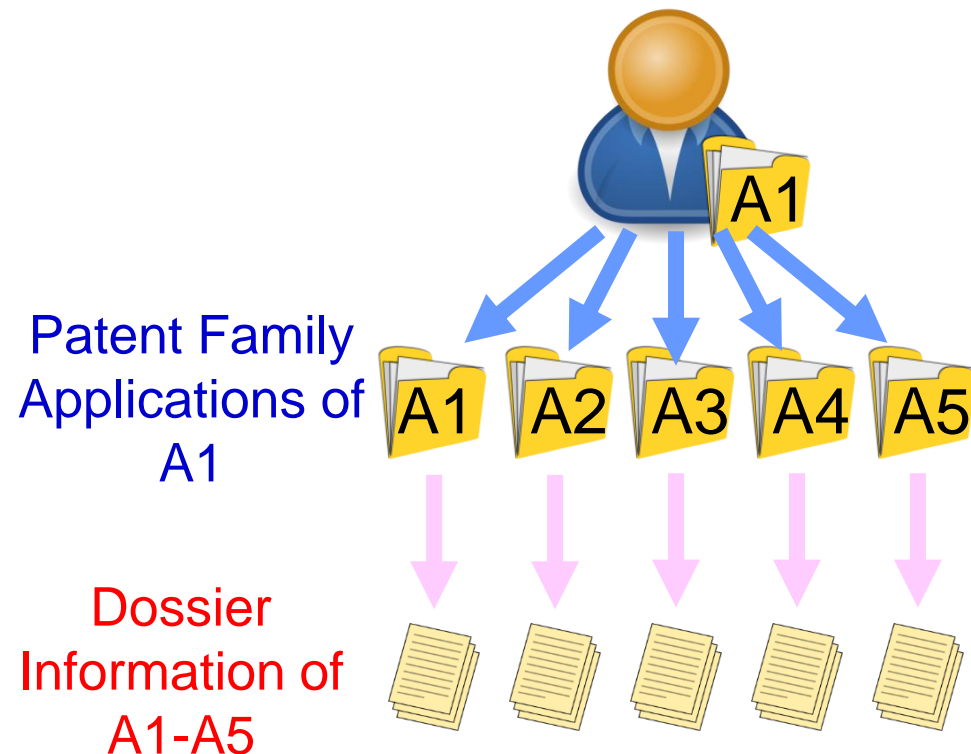
- Background
- **WIPO CASE Service**
- Functions of WIPO CASE
- Future Development

# WIPO CASE Service - Outline

In order to retrieve **dossier information** of **patent family applications** ...

- ① Find patent family applications  
(Patent family search)
- ② Access dossier information of them

**WIPO CASE Service**





# WIPO CASE Service - Outline

- Patent family search
  - Find patent family applications
- Dossier information access
  - See prosecution history *e.g. filing, office action, amendment, decision, etc.*
  - Read dossier contents
    - File wrapper documents (original/translated)  
*e.g. Original/amended claims, Office actions, Arguments, etc.*
    - Bibliographic information  
*e.g. Application/publication number, Application/publication date, etc.*
    - Citation information *e.g. Publication number of cited patent document, etc.*
  - Compare file wrapper documents  
*e.g. 1st claims vs. 2nd claims, Claims vs. Office action, Claims in office A vs. Claims in office B, Office action in office A vs. Office action in office B etc.*
  - Read patent documents (original/translated)  
*e.g. Patent family application document, Cited patent document, etc.*
  - Access dossier information in a timely manner  
*e.g. Access dossier information when an office action is sent to the applicant, etc.*

# WIPO CASE Service - Outline

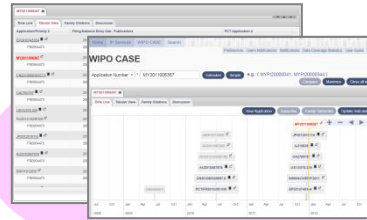
Various features can be used on the **WIPO CASE Portal**.

- Patent family search -> Simple Search / Extended Search  
-> Time Line View / Tabular View
- Dossier information access
  - Prosecution history -> Document List
  - Dossier contents
    - File wrapper documents (original/translated)  
-> Document Viewer/Downloader
    - Bibliographic information -> Bibliographic Data
    - Citation information -> Citation Data / Family Citation
  - Comparison of file wrapper documents  
-> Document Comparison View (*Documents are shown side by side*)
  - Access to patent documents (original/translated)  
-> Link to PATENTSCOPE  
-> Search for patent family of cited patent
  - Timeliness -> Notification

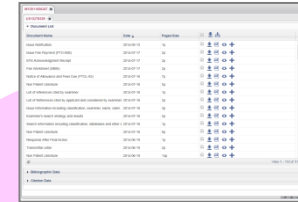
# WIPO CASE Service - Outline



Notification



Patent family search

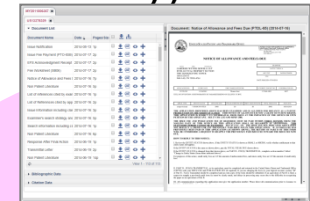


Document List  
(Prosecution history)

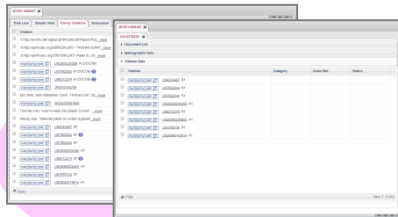


Patent document  
& translation

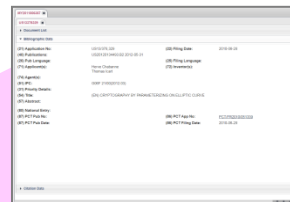
Improve  
**Efficiency** and **Quality**  
of Examination



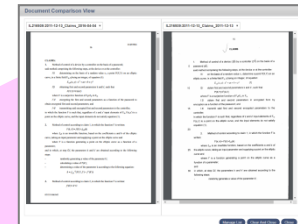
File wrapper document  
& translation



Citation Information



Bibliographic Information



Document comparison

# WIPO CASE Service – Patent Family

## ■ Patent Family Data

- National applications and PCT applications
  - Application (number and date)
  - Publication (number, dates and kind code)
  - Priority application (number and date)
  - National phase entry application (number and date)
- Coverage
  - 52 offices (including many of Providing Offices and Accessing Offices, etc.)
- Data coverage information updated daily

# WIPO CASE Service – Patent Family

- More than 30 million applications from 52 offices

Offices				
AU	CA	CN	EP	GB
IL	JP	KR	US	WO
AE	AR	BH	BN	BR
CL	CO	CR	CU	DD
DE	DO	EA	EC	EE
EG	ES	FR	GT	HN
ID	IN	JO	KE	KH
MA	MN	MX	MY	NI
PA	PE	PH	PT	RU
SG	SU	SV	TH	TN
VN	ZA			

# WIPO CASE Service - Document Data

Office	AU*	CA	CN*	EP*	GB*	IL	JP*	KR*	US*	IB
Applications published since	Jan 1, 2006	Jan 1, 2008			Jan 1, 2008					Jan 1, 1978
Published applications that are filed on and after			Feb 10, 2010	Jan 1, 1990		Jan 1, 2010	Dec 1, 1990	Jan 1, 1999	Jan 1, 2003	
Specifications and Incoming Documents (e.g. claims, amendment)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Outgoing Documents (e.g. examination document)	Yes	Yes	Yes**	Yes	Yes	Yes**	Yes**	Yes**	Yes	Yes**

ORGANIZATION

\*: Citation provided, \*\*: Including translation

# Example of Useful Document (1)

- When referring to dossier information, examiners often check original/amended claims, citations, search/examination reports and applicants' opinions.
- Such information is mainly contained in the following documents.

Office	AU	CA	CN	EP
Original claims Amended claims Applicant's opinion	Claims exrs	Claims Amendment	Invention Publication Claims Argument	Claims Amended claims Amendments received before examination Reply to communication from the Examining Division
Citations Search report Examination report	Examination report	R30(2)Examiner requisition	First Office Action Nth Office Action Notification to Grant Patent Right for Invention	European search report European search opinion Communication from the Examining Division (with annex) Text intended for grant Decision to refuse the application (with annex)

# Example of Useful Document (2)

Office	GB	IL	JP	KR
<b>Original claims</b> <b>Amended claims</b> <b>Applicant's opinion</b>	A spec Claims Specifications	Claims	Claims Written Amendment Written Argument	Patent Application Paper according to the Article 203 of Patent Act Document under Articles 201 and 203 of Patent Act Amendment Written Opinion
<b>Citations</b> <b>Search report</b> <b>Examination report</b>	Exam report search stage Exam opinion search stage Further search report Search Statement Examination report	Article 15(5) search report Examination report	Notification of Reasons for Refusal Decision to Grant a Patent Decision of Refusal	Notification of Reason for Refusal (Request for the Submission of an Opinion) Final Office Action Written Decision on Registration Notice of Final Rejection



# Example of Useful Document (3)

Office	US	IB
Original claims	Claims	
Amended claims	Applicant Arguments/Remarks Made in an Amendment	Application Body (Translation of IA Body)
Applicant's opinion	Response to Election / Restriction Filed	
Citations	Non-Final Rejection	International Search Report
Search report	Notice of Allowance and Fees Due (PTOL-85)	Written Opinion of the International Search Authority
Examination report	Final Rejection	International Preliminary Report on Patentability Chapter I
	Requirement for Restriction/Election	International Preliminary Report on Patentability Chapter II (IPEA/409) <sup>1</sup>

1. IPRP II includes amended claims, too.

- Please note that these documents are just examples. Sometimes other documents also contain this information.

# Possible Scene for Use of WIPO CASE

## ■ Example of examination procedure

### Understanding

- Subject matter
  - Background
- ✓ Collect patent family information and check its relevance

### Search

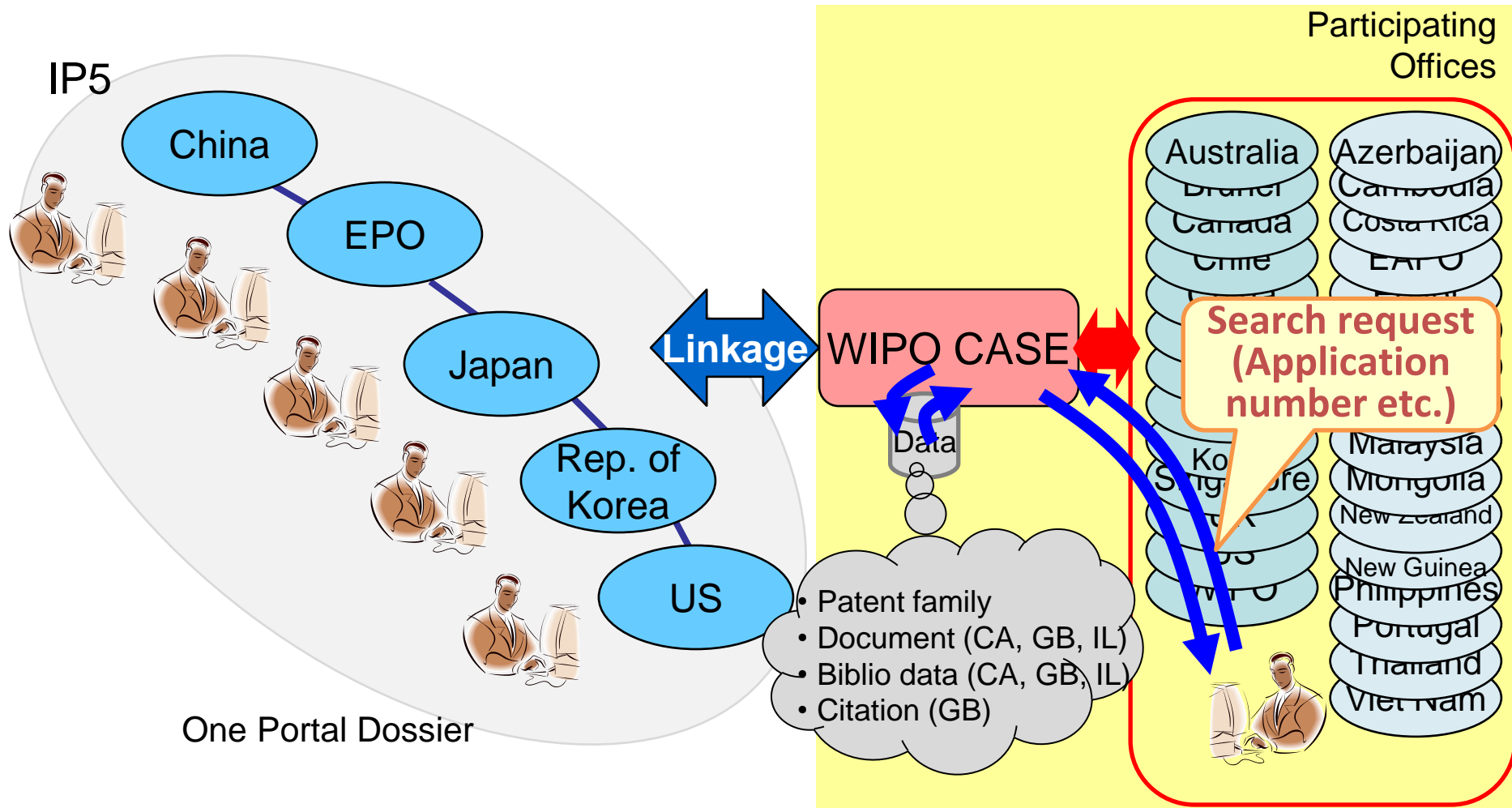
- Prior Art
- ✓ Check claim differences, citations of patent family members
  - ✓ Check patent families of citations or their own prior arts

### Examination

- Drafting
  - Communication with applicant
- ✓ Check examination document, amended claims, applicant's opinions or history of patent family members

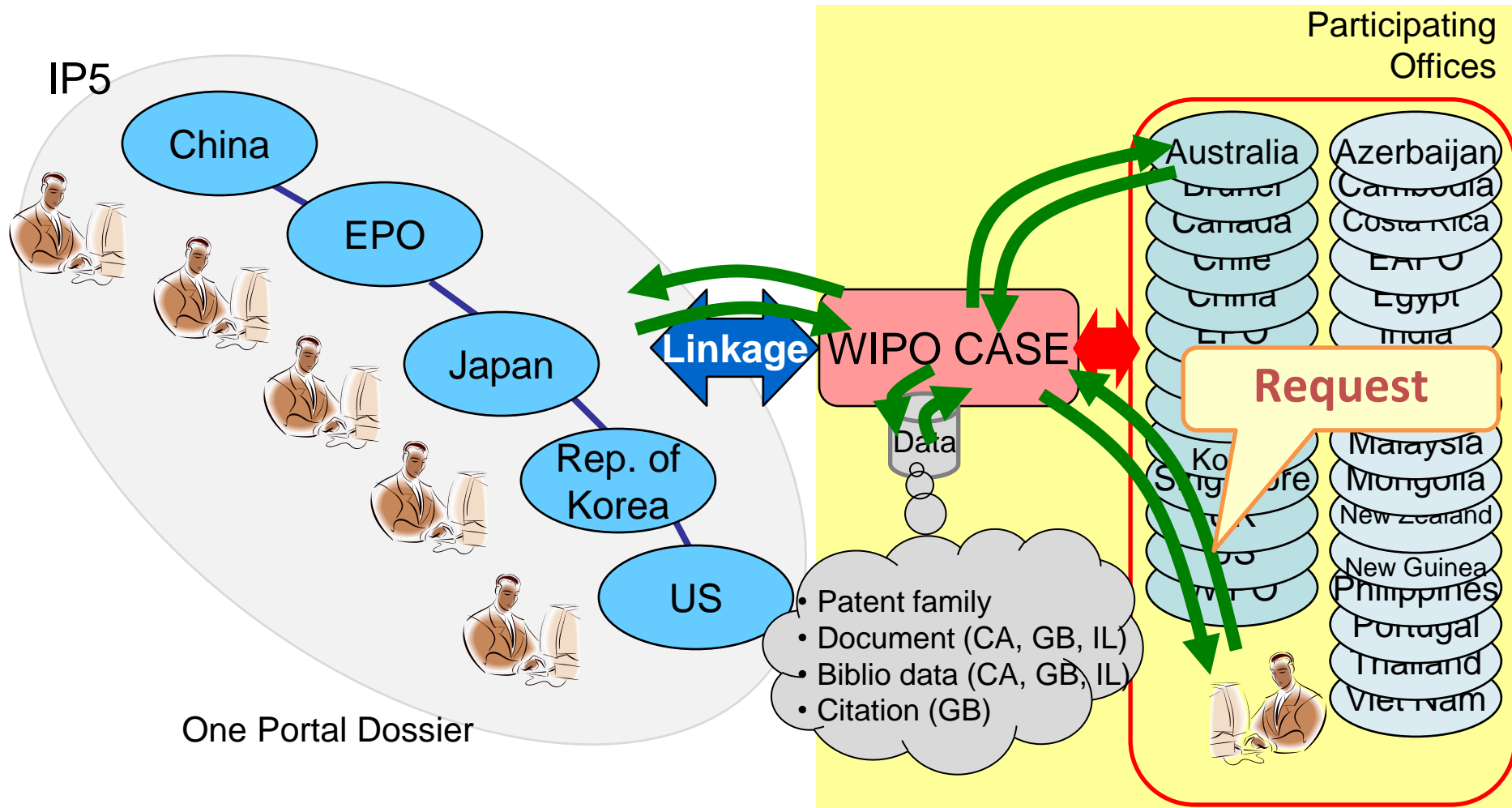
# WIPO CASE Service – How It Works

## ■ Patent family search



# WIPO CASE Service – How It Works

## ■ Dossier information Access



# Advantage

- One portal to access dossier information from many providing offices
  - Currently 10 offices (IP5 + AU, CA, GB, IL, WO)
  - Providing offices are continuously increasing
  
- Broad data coverage of patent family information
  - Currently across 52 offices
  - Data coverage is continuously expanding
  
- Powerful user interface
  - Many features which support examination

# Outline

- Background
- WIPO CASE Service
- **Functions of WIPO CASE**
- Future Development

# Functions of WIPO CASE

## ■ WIPO CASE Web Portal

- Time Line View (Patent Family Search)
- Document List
- Viewing/Downloading Documents
- Bibliographic/Citation Data
- Translation
- Comparison of Documents
- Tabular View
- Family Citations
- Notification Service
- Configurable User Preference
- User Guide

# Note

When you use WIPO CASE, please note the followings:

- You can use WIPO CASE on your web browser. If some features don't work well, please change your browser.
- You might get disconnected in about 30 minutes depending on the load condition. If disconnected, you need to sign in again.



# Sign in

<http://www.wipo.int/case/en/>

**WIPO** Contact Us English ▾

Home › IP Services

## Sign in

Username   
[Forgot your username?](#)

Password   
[Forgot your password?](#)

**Sign in**

**Don't have a WIPO Account?**  
[Create account](#)

**Why create a WIPO Account?**  
 Using just one username and password, you can access your profiles for any of the following services:

- PCT
- Madrid system
- Hague system
- WIPO Green

Registration for the WIPO account is open to all users and free of charge.

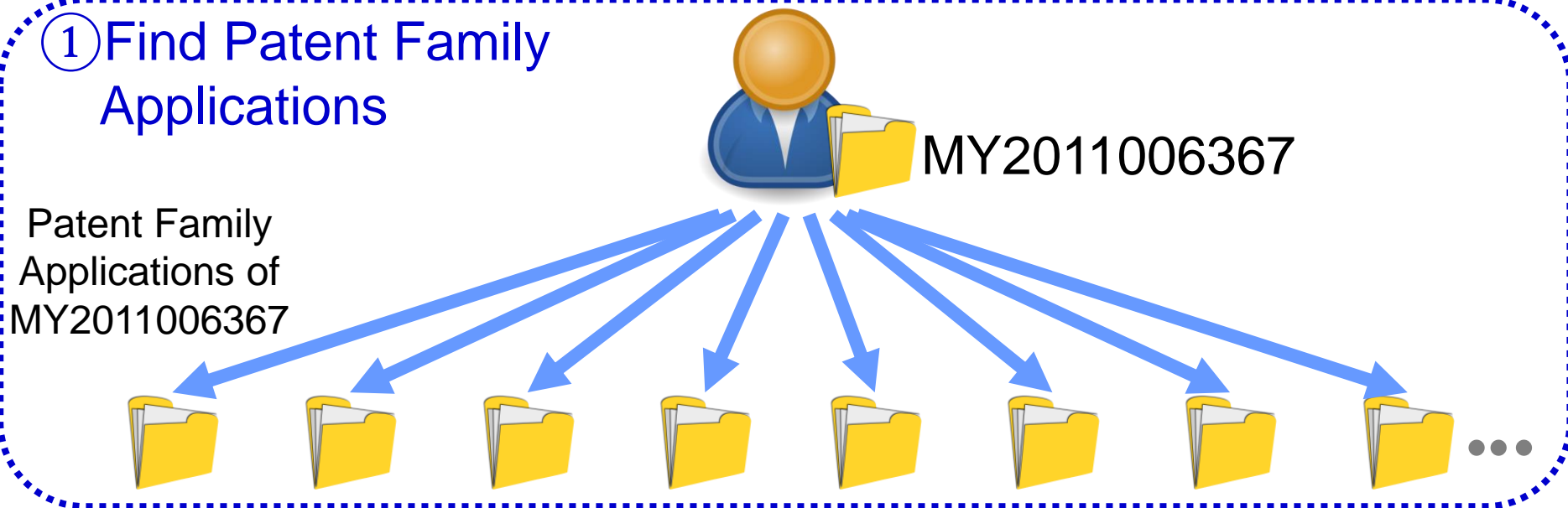
**Having difficulties?**  
[Read our WIPO Account help guide.](#)  
 during 2012 and is now operational for exchange of documents between examiners in the three offices.

Since June 1, 2015, any patent office may join the system by notifying the International

**ERTY**

# Patent Family Search

## ① Find Patent Family Applications



# Time Line View (Patent Family Search)

**App**

**ew ily)**

**Machine translation**

**Application**

**MY201100**

**Time Line**

**PermaLink**

**icators**

**Oct**

**ACTUAL PROPERTY ATION**

**WIPO PATENTSCOPE**

Search International and National Patent Collections

WORLD INTELLECTUAL PROPERTY ORGANIZATION

Search Browse Translate Options News Login Help

Home > IP Services > PATENTSCOPE

1. (US20120134493) Cryptography by parameterizing on elliptic curve

National Biblio. Data Description Claims Drawings Documents

Application Number: 13378329 Application Date: 28.06.2010  
 Publication Number: 20120134493 Publication Date: 31.05.2012  
 Grant Number: 08824670 Grant Date: 02.09.2014  
 Publication Kind : B2  
 Prior PCT appl.: Application Number:PCTFR2010051339 ; Publication Number: Click to see the data

IPC: G06F 21/00 CPC: H04L 9/3066  
 H04L 9/00 H04L 9/005  
 H04L 9/30 H04L 9/0844  
 H04L 9/08 H04L2209/08

Applicants: Icart Thomas  
 Morpho  
 Chabanne Herve

Inventors: Icart Thomas  
 Chabanne Herve

Agents: Gardere Wynne Sewell LLP  
 Szuwalski Andre M.

Priority Data: 09 54473 30.06.2009 FR

Title: (EN) Cryptography by parameterizing on elliptic curve

Abstract: (EN)  
 A device is controlled by a controller on the basis of a password. A determination is made at the device or at the controller, on the basis of a random value  $r_1$ , of a point  $P(X,Y)$  on an elliptic curve in a finite body  $F_q$ ,  $q$  being an integer, according to:  $E_{a,b}(x, y):x^3+ax+by^2$ . First and second parameters  $k$  and  $k'$  are obtained such that  $P(X,Y)=F(K,k')$ , where  $F$  is a surjective function of  $F_q \times F_q$  in  $F_q$ . The first and second parameters are obtained in an encrypted format by encryption in accordance with the password. The first and second encrypted parameters are then transmitted to the controller. During the control, the function  $F$  is used, such that, whatever the values of  $z$  and  $z'$  which are input elements of  $F_q$ ,  $F(z,z')$  is a point on the elliptic curve and the input elements do not satisfy the equation.

Jul 2008

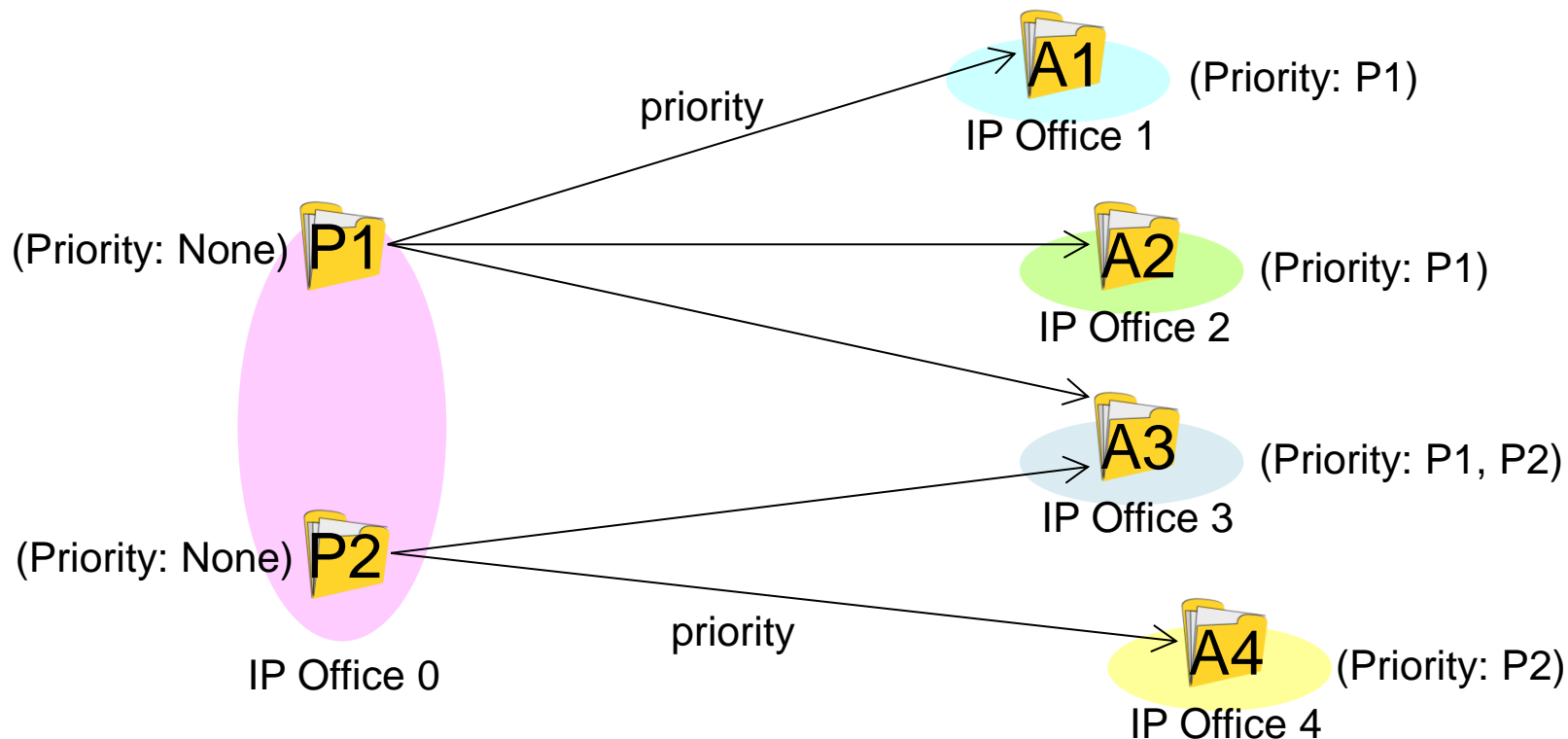
# Patent Family Search

## ■ Patent Family Search

- Simple search
  - One level backward and then one level forward
  
- Extended search
  - All sets of applications related by priority or national phase entry

# Patent Family Search

## ■ Example of Patent Family Search



→ Search for the patent family applications

# Patent Family Search

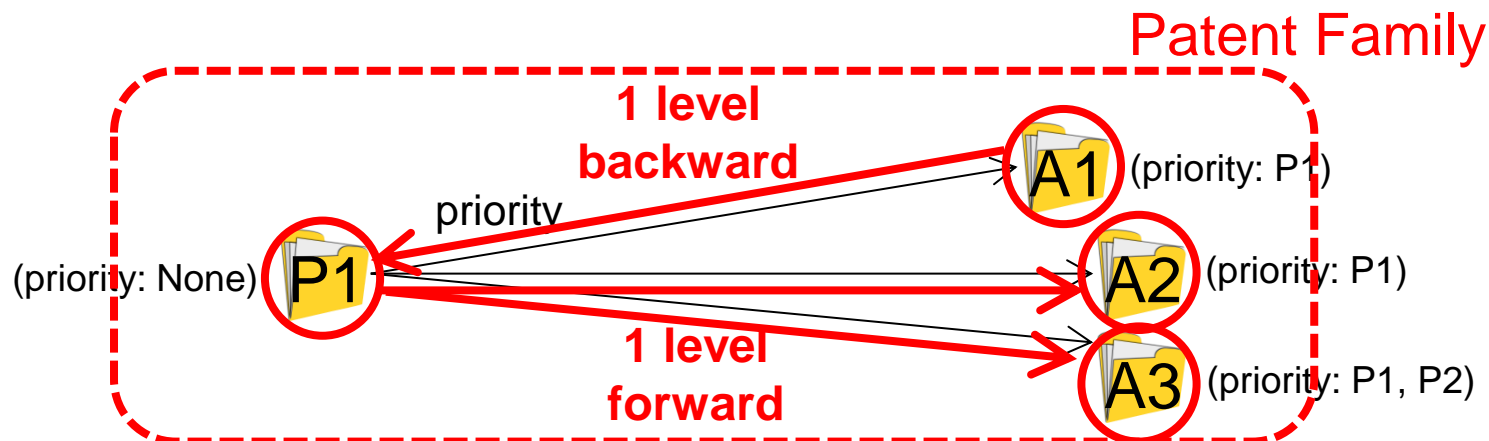
## ■ Example of Patent Family Search

### Patent family of A1

#### ➤ Simple search

- One level backward and then one level forward

→ A1, P1, A2, A3



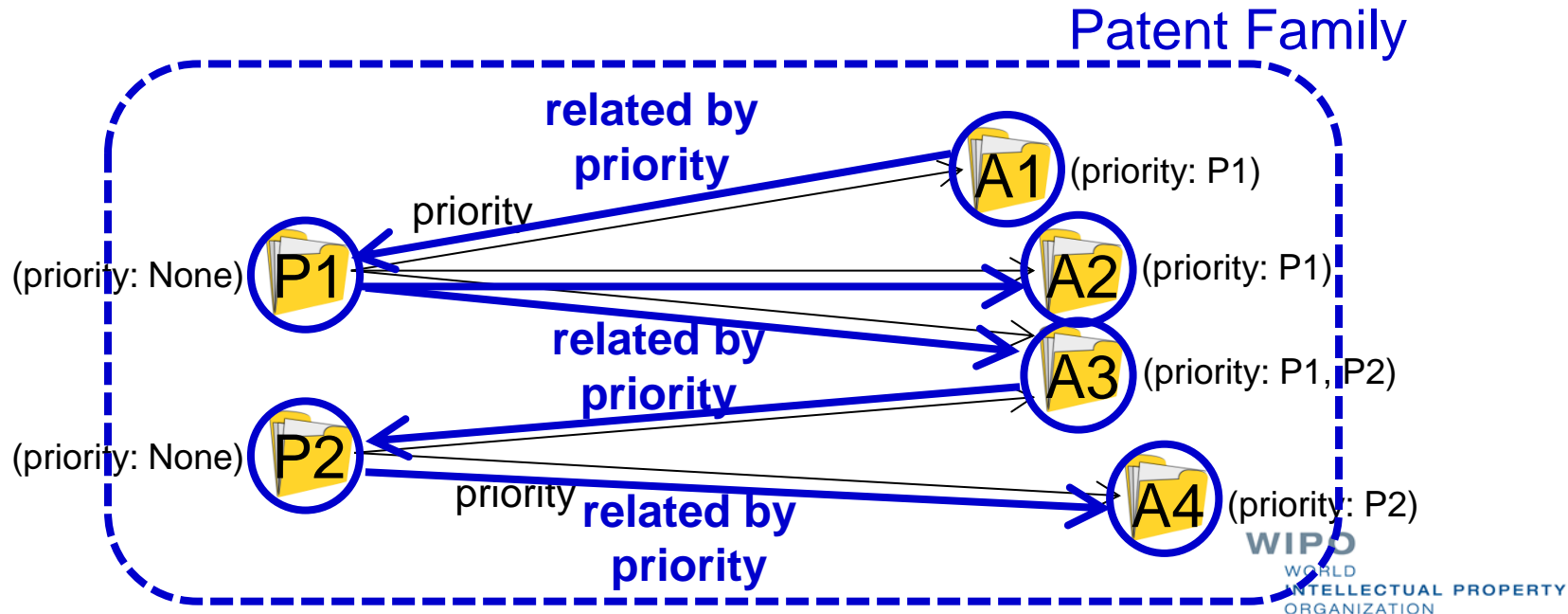
# Patent Family Search

## ■ Example of Patent Family Search

### Patent family of A1

#### ➤ Extended search

- All sets of applications related by priority or national phase entry  
→ A1, P1, A2, A3, P2, A4



# Patent Family Search

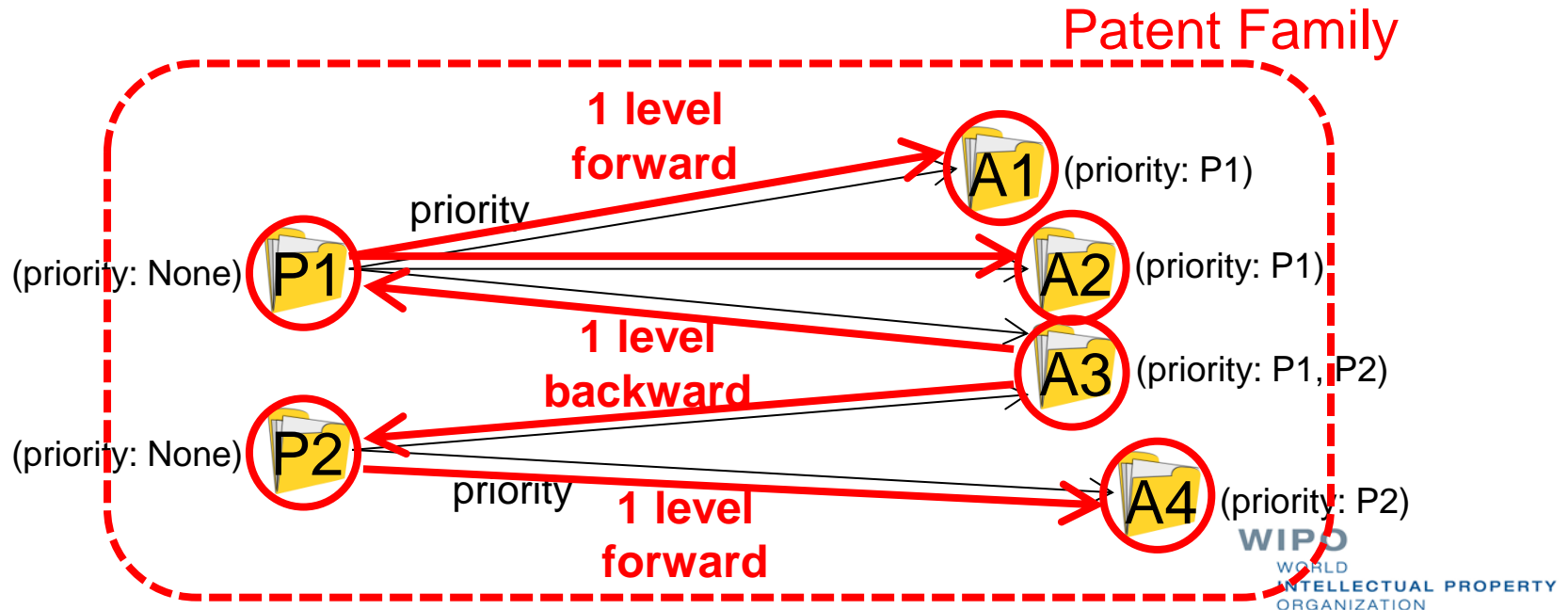
## ■ Example of Patent Family Search

### Patent family of A3

#### ➤ Simple search

- One level backward and then one level forward

→ A3, P1, P2, A1, A2, A4





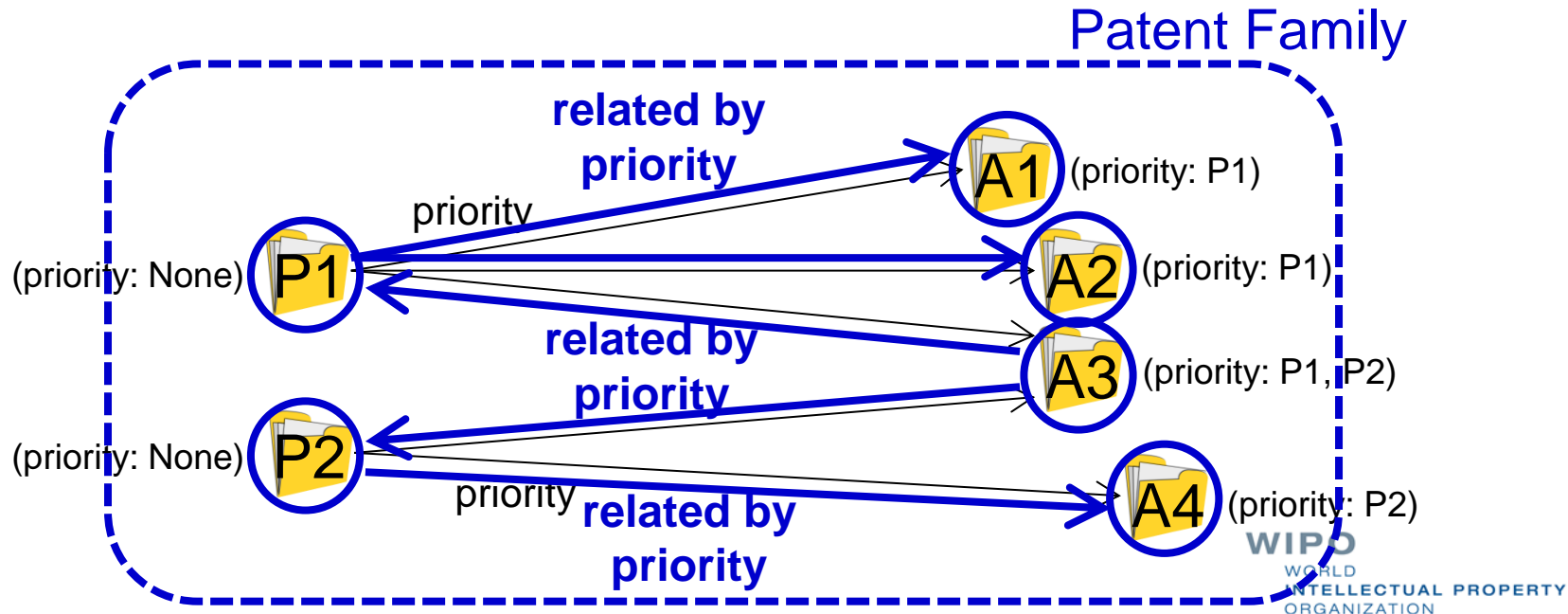
# Patent Family Search

## ■ Example of Patent Family Search

### Patent family of A3

#### ➤ Extended search

- All sets of applications related by priority or national phase entry  
→ A3, P1, P2, A1, A2, A4



# Patent Family Search

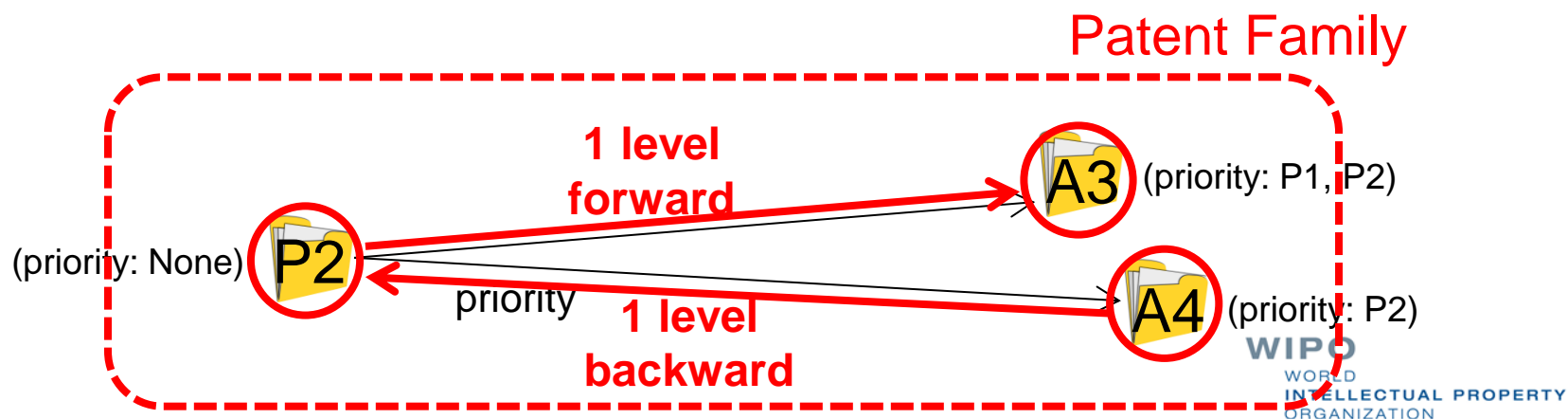
## ■ Example of Patent Family Search

### Patent family of A4

#### ➤ Simple search

- One level backward and then one level forward

→ A4, P2, A3



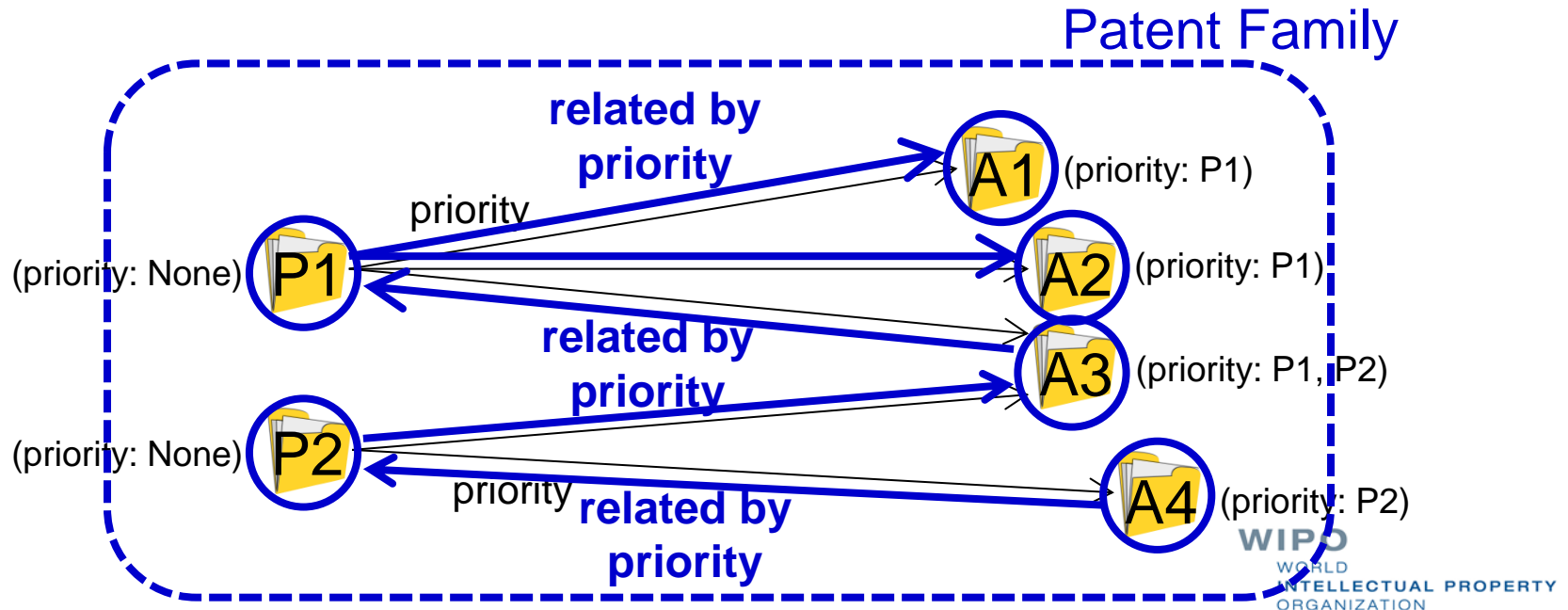
# Patent Family Search

## ■ Example of Patent Family Search

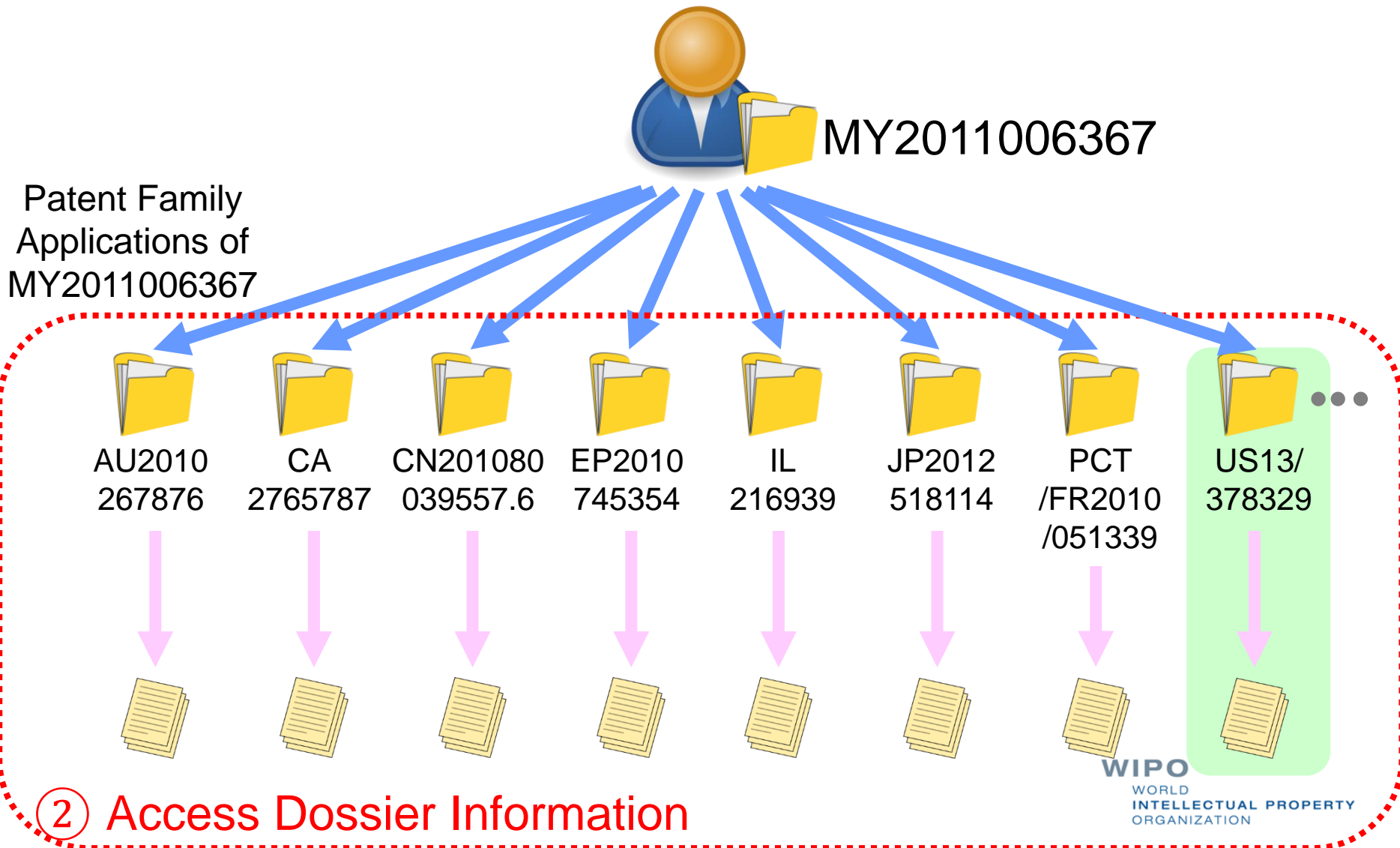
### Patent family of A4

#### ➤ Extended search

- All sets of applications related by priority or national phase entry  
→ A4, P2, A3, P1, A1, A2



# Retrieving Dossier Information



# Document List (1)

MY2011006367 x

US13378329 x

▼ Document List

Document Name	Date	Pages/Size	
Issue Notification	2014-08-13	1p	<input type="checkbox"/>
Issue Fee Payment (PTO-85B)	2014-07-17	2p	<input type="checkbox"/>
EFS Acknowledgment Receipt	2014-07-17	2p	<input type="checkbox"/>
Fee Worksheet (SB06)	2014-07-17	2p	<input type="checkbox"/>
Notice of Allowance and Fees Due (PTOL-85)	2014-07-16	7p	<input type="checkbox"/>
Non Patent Literature	2014-07-16	5p	<input type="checkbox"/>
List of references cited by examiner	2014-07-16	1p	<input type="checkbox"/>

View 1 - 113 of 113

► Bibliographic Data

► Citation Data

Time Line Tabular View Family Citations Discussion

View Application Subscribe Family Subscribe Update Indicators

BRP11012658

SG2011097052

MY2011006367

JP2012518114

IL216939

**Document List  
(Prosecution History)**

# Document List (2)

MY2011006367 x

US13378329 x

▼ Document List

Document Name	Date	Pages/Size	
Issue Notification	2014-08-13	1p	<input type="checkbox"/>
Issue Fee Payment (PTO-85B)	2014-07-17	2p	<input type="checkbox"/>
EFS Acknowledgment Receipt	2014-07-17	2p	<input type="checkbox"/>
Fee Worksheet (SB06)	2014-07-17	2p	<input type="checkbox"/>
Notice of Allowance and Fees Due (PTOL-85)	2014-07-16	7p	<input type="checkbox"/>
Non Patent Literature	2014-07-16	5p	<input type="checkbox"/>
List of references cited by examiner	2014-07-16	1p	<input type="checkbox"/>

View 1 - 113 of 113

► Bibliographic Data

► Citation Data

Time Line Tabular View Family Citations Discussion

View Application Subscribe Family Subscribe Update Indicators

BRP11012658

SG2011097052

MY2011006367

JP2012518114

IL216939

**Document List  
(Prosecution History)**

# Viewing/Downloading Documents

**Download**

Document Name	Date	Pages/Size			
Issue Notification	2014-08-13	1p			
Issue Fee Payment (PTO-85B)	2014-07-17	2p			
EFS Acknowledgment Receipt	2014-07-17	2p			
Fee Worksheet (SB06)	2014-07-17	2p			
Notice of Allowance and Fees Due (PTOL-85) (2014-07-16)	2014-07-16	7p			
Non Patent Literature	2014-07-16	5p			
List of references cited by examiner	2014-07-16	1p			
List of References cited by applicant	2014-07-16	2p			
Issue Information including classification	2014-07-16	3p			
Examiner's search strategy and search	2014-07-16	5p			
Search information including classification	2014-07-16	1p			
Non Patent Literature	2014-07-16	6p			
Response After Final Action	2014-06-19	1p			
Transmittal Letter	2014-06-19	2p			
Non Patent Literature	2014-06-19	14p			

View 1 - 113 of 113

[Bibliographic Data](#)  
[Citation Data](#)

**Document: Notice of Allowance and Fees Due (PTOL-85) (2014-07-16)**

**Document: Notice of Allowance and Fees Due (PTOL-85) (2014-07-16)**

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: C/COMMERCIAL/PTO PATENT CENTER  
 P.O. Box 1455  
 Alexandria, Virginia 22313-1455  
 www.uspto.gov

**NOTICE OF ALLOWANCE AND FEE(S) DUE**

EXAMINER  
 BAYOU, YONAS A

ART UNIT  
 PAPER NUMBER  
 2404

DATE MAILED: 07/16/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/078,329	12/14/2011	Thomas Icart	137660-1005	9057

TITLE OF INVENTION: CRYPTOGRAPHY BY PARAMETERIZING ON ELLIPTIC CURVE

APPL. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEES DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$960	\$0	\$0	\$960	10/16/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

**HOW TO REPLY TO THIS NOTICE:**

1. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEES DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEES) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

If the ENTITY STATUS is changed from that shown above, on PART B - FEES) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

If the ENTITY STATUS is changed from that shown above, on PART B - FEES) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

**Document**

WORKED IN PART BY THE INTELLECTUAL PROPERTY ORGANIZATION

# Display Mode (1)

MY2011006367 x

US13378329 x

Document List

Document Name	Date	Pages/Size	<input type="checkbox"/>	↓	PDF	○	+
Issue Notification	2014-08-13	1p	<input type="checkbox"/>	↓	PDF	○	+
Issue Fee Payment (PTO-85B)	2014-07-17	2p	<input type="checkbox"/>	↓	PDF	○	+
EFS Acknowledgment Receipt	2014-07-17	2p	<input type="checkbox"/>	↓	PDF	○	+
Fee Worksheet (SB06)	2014-07-17	2p	<input type="checkbox"/>	↓	PDF	○	+
Notice of Allowance and Fees Due (PTOL-85)	2014-07-16	7p	<input type="checkbox"/>	↓	PDF	○	+
Non Patent Literature	2014-07-16	5p	<input type="checkbox"/>	↓	PDF	○	+
List of references cited by examiner	2014-07-16	1p	<input type="checkbox"/>	↓	PDF	○	+
List of References cited by applicant and considered by examiner	2014-07-16	2p	<input type="checkbox"/>	↓	PDF	○	+
Issue Information including classification, examiner, name, claim,	2014-07-16	3p	<input type="checkbox"/>	↓	PDF	○	+
Examiner's search strategy and results	2014-07-16	5p	<input type="checkbox"/>	↓	PDF	○	+
Search information including classification, databases and other s	2014-07-16	1p	<input type="checkbox"/>	↓	PDF	○	+
Non Patent Literature	2014-07-16	6p	<input type="checkbox"/>	↓	PDF	○	+
Response After Final Action	2014-06-19	1p	<input type="checkbox"/>	↓	PDF	○	+
Transmittal Letter	2014-06-19	2p	<input type="checkbox"/>	↓	PDF	○	+
Non Patent Literature	2014-06-19	14p	<input type="checkbox"/>	↓	PDF	○	+

View 1 - 113 of 113

▶ Bibliographic Data

▶ Citation Data



# Display Mode (2)

MY2011006367 x

US13378329 x

▼ Document List

Document Name	Date ↓	Pages/Size	<input type="checkbox"/> ↓ PDF
Issue Notification	2014-08-13	1p	<input type="checkbox"/> ↓ PDF ○ +
Issue Fee Payment (PTO-85B)	2014-07-17	2p	<input type="checkbox"/> ↓ PDF ○ +
EFS Acknowledgment Receipt	2014-07-17	2p	<input type="checkbox"/> ↓ PDF ○ +
Fee Worksheet (SB06)	2014-07-17	2p	<input type="checkbox"/> ↓ PDF ○ +
Notice of Allowance and Fees Due (PTOL-85)	2014-07-16	7p	<input type="checkbox"/> ↓ PDF ○ +
Non Patent Literature	2014-07-16	5p	<input type="checkbox"/> ↓ PDF ○ +
List of references cited by examiner	2014-07-16	1p	<input type="checkbox"/> ↓ PDF ○ +
List of References cited by applicant and considered by examiner	2014-07-16	2p	<input type="checkbox"/> ↓ PDF ○ +
Issue Information including classification, examiner, name, claim,	2014-07-16	3p	<input type="checkbox"/> ↓ PDF ○ +
Examiner's search strategy and results	2014-07-16	5p	<input type="checkbox"/> ↓ PDF ○ +
Search information including classification, databases and other s	2014-07-16	1p	<input type="checkbox"/> ↓ PDF ○ +
Non Patent Literature	2014-07-16	6p	<input type="checkbox"/> ↓ PDF ○ +
Response After Final Action	2014-06-19	1p	<input type="checkbox"/> ↓ PDF ○ +
Transmittal Letter	2014-06-19	2p	<input type="checkbox"/> ↓ PDF ○ +
Non Patent Literature	2014-06-19	14p	<input type="checkbox"/> ↓ PDF ○ +

View 1 - 113 of 113

► Bibliographic Data

► Citation Data

# Bibliographic Data

MY2011006367 x

US13378329 x

Document List

Bibliographic Data

(21) Application No:	US13/378,329	(22) Filing Date:	2010-06-28
(40) Publications:	US20120134493.B2 2012-05-31	(25) Filing Language:	
(26) Pub Language:		(72) Inventor(s):	
(71) Applicant(s):	Herve Chabanne Thomas Icart		
(74) Agent(s):			
(51) IPC:	G06F 21/00(2012.03)		
(31) Priority Details:			
(54) Title:	(EN) CRYPTOGRAPHY BY PARAMETERIZING ON ELLIPTIC CURVE		
(57) Abstract:			
(85) National Entry:			
(87) PCT Pub No:		(86) PCT App No:	<a href="#">PCT/FR2010/051339</a>
(87) PCT Pub Date:		(86) PCT Filing Date:	2010-06-28

Citation Data

**Bibliographic Data**

# Citation Data (1)

**WIPO PATENTSCOPE**  
 Search International and National Patent Collections

WORLD INTELLECTUAL PROPERTY ORGANIZATION

Search Browse Translate Options News Login Help

Home > IP Services > PATENTSCOPE

**Machine translation**

1 (US6243467) Method of elliptic curve cryptographic digital signature generation and verification using reduced base tau expansion in non-adjacent form

National Biblio. Data Description Claims Drawings Documents

PermaLink

**Application Number:** 09120740 **Application Date:** 23.07.1998  
**Publication Number:** 6243467 **Publication Date:** 05.06.2001  
**Grant Number:** 6243467 **Grant Date:** 05.06.2001  
**Publication Kind :** B1

**IPC:** H04L 9/30 CPC: G06F 7/725  
 H04L 9/32 H04L 9/3066  
 H04L 9/3247

**Applicants:** The United States of America as represented by the National Security Agency  
**Inventors:** Reiter, Robert W.  
 Solinas, Jerome A.  
**Agents:** Morelli, Robert D.  
**Priority Data:** 09120740 23.07.1998 US  
**Title:** (EN) Method of elliptic curve cryptographic digital signature generation and verification using reduced base tau expansion in non-adjacent form  
**Abstract:** (EN)

A method of generating and verifying a digital signature by selecting an elliptic curve; selecting a point G; generating x and M; reducing x; generating a base tau expansion, in non-adjacent form, of the reduced x; multiplying G by the expansion; computing  $h = \text{Hash}(M)$ ; generating k; reducing k; generating a base tau expansion, in non-adjacent form, of the reduced k; multiplying G by the expansion of k to form  $K = (K_x, K_y)$ ; computing  $R = (K_x \text{ mod } q)$ ; returning to the step of generating k if  $R=0$ , otherwise computing  $S = (k \text{ circumflex over } ( ) - 1)(h + xR)$ ; returning to the step of generating k if  $S=0$ , otherwise transmitting y, q, M, R, and S; receiving y, q, M, R, and S; proceeding with the next step if  $0 < R < q$  and  $0 < S < q$ , otherwise not verifying the digital signature and stopping; forming  $h = \text{Hash}(M)$ ; computing  $f = (S \text{ circumflex over } ( ) - 1) \text{ mod } n$ ;  $b = (hf \text{ mod } n)$ ; and  $t = (Rf \text{ mod } n)$ ; reducing b and t

- 1 USER A PICKS AN ELLIPTIC CURVE AND A BASE POINT G ON THE ELLIPTIC CURVE
- 2 USER A GENERATES A SIGNATURE KEY x AND A MESSAGE M
- 3 USER A REDUCES x AND GENERATES A TAU-ADIC EXPANSION OF REDUCED x IN NON-ADJACENT FORM
- 4 USER A MULTIPLIES G BY THE TAU-ADIC EXPANSION OF REDUCED x TO FORM A POINT y ON THE ELLIPTIC CURVE
- 5 USER A FORMS A HASH h OF THE MESSAGE
- 6

Copy

JP2005083222

Status

Currently Available for AU, CN, EP, GB, JP, KR, US

# Citation Data (2)

The screenshot displays a patent database interface with the following elements:

- Tab: MY2011006367
- Tab: US13378329
- Section: Document List
- Section: Bibliographic Data
- Section: Citation Data
- Section: Citations (Dialog Box)

The Citations dialog box contains the following list of patents:

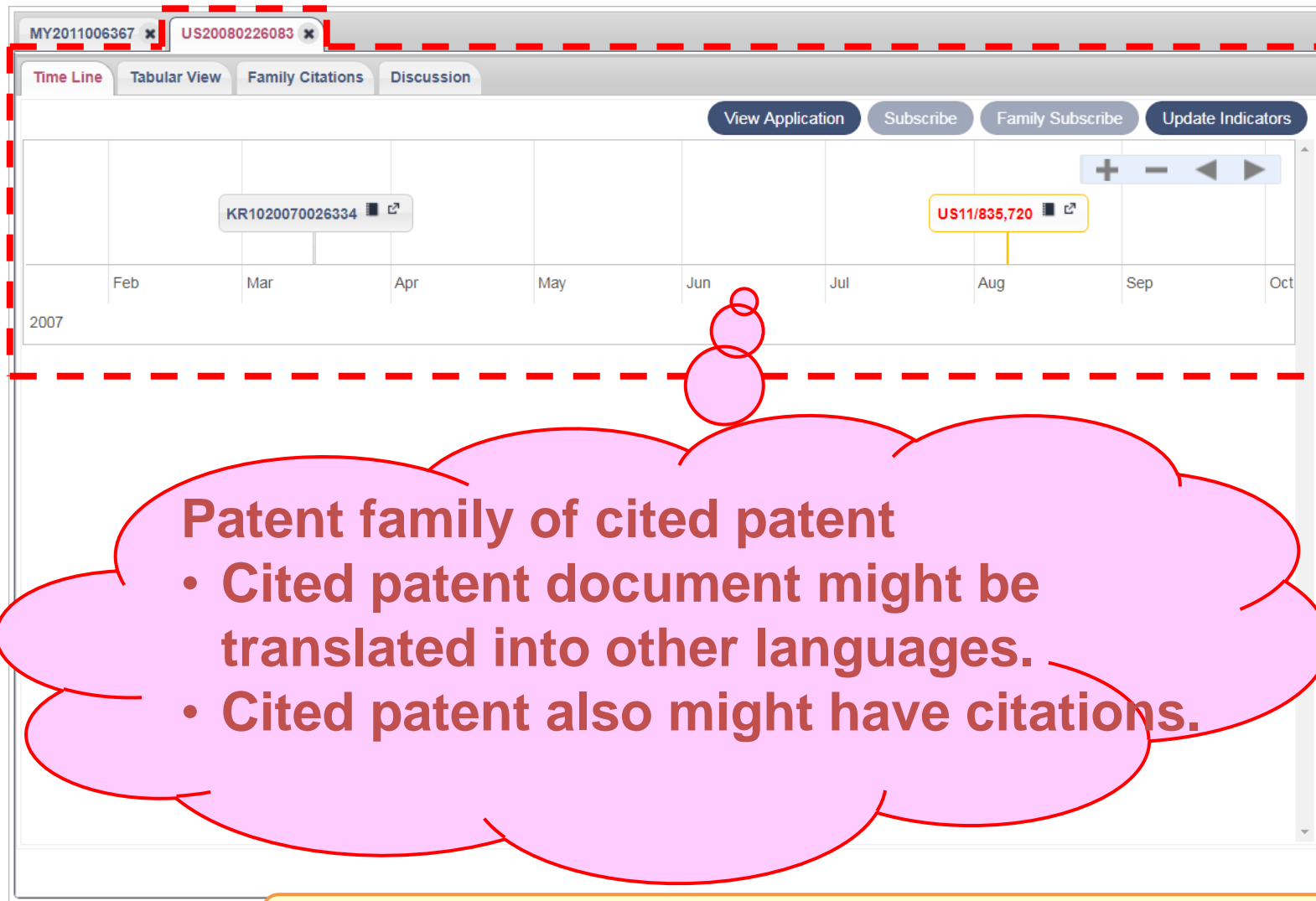
US6243467 B1
US7062044 B1
US7062043 B1
US20030235300 A1
US6212279 B1

The 'Ok' button in the dialog box is highlighted with a red arrow. A red arrow also points to the 'Citation Data' section in the main interface.

Copy View 1 - 8 of 8

Currently Available for AU, CN, EP, GB, JP, KR, US

# Citation Data (3)



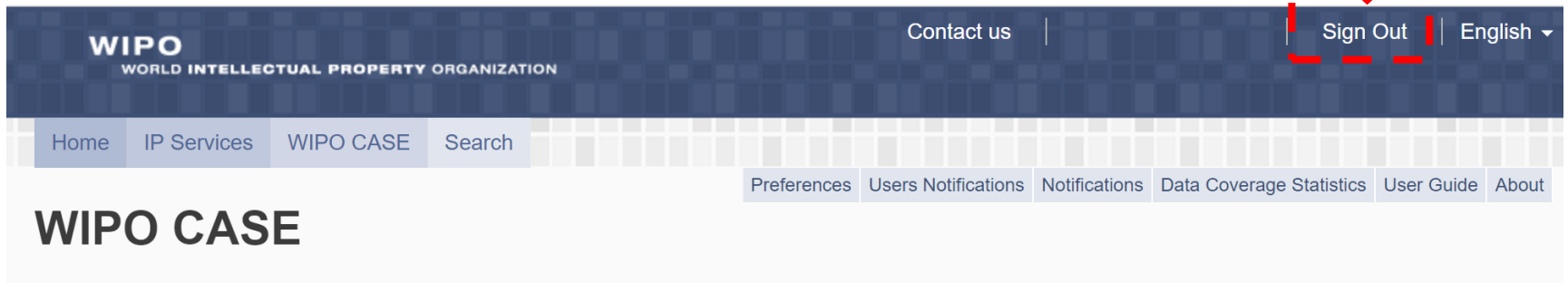
Currently Available for AU, CN, EP, GB, JP, KR, US

# Close Tab

The screenshot displays a web application interface for patent data. At the top, there are two tabs: 'MY2011006367' and 'US13378329'. Below the tabs, there is a 'Document List' section with three expandable items: 'Document List', 'Bibliographic Data', and 'Citation Data'. The 'Citation Data' section is expanded, showing a table with the following columns: Citation, Category, Calim-Ref, and Status. The table contains 8 rows of data, each starting with a 'PATENTSCOPE' link and a patent number followed by a classification code. At the bottom left, there is a 'Copy' button, and at the bottom right, it says 'View 1 - 8 of 8'.

Citation	Category	Calim-Ref	Status
<a href="#">PATENTSCOPE</a> <a href="#">US6243467</a> B1			
<a href="#">PATENTSCOPE</a> <a href="#">US7062044</a> B1			
<a href="#">PATENTSCOPE</a> <a href="#">US7062043</a> B1			
<a href="#">PATENTSCOPE</a> <a href="#">US20030235300</a> A1			
<a href="#">PATENTSCOPE</a> <a href="#">US6212279</a> B1			
<a href="#">PATENTSCOPE</a> <a href="#">US20080226083</a> A1			
<a href="#">PATENTSCOPE</a> <a href="#">US7970134</a> B1			
<a href="#">PATENTSCOPE</a> <a href="#">US20040119614</a> A1			

# Sign out



The image shows the top navigation bar of the WIPO CASE website. The bar has a dark blue background with a grid pattern. On the left, the WIPO logo is displayed above the text "WORLD INTELLECTUAL PROPERTY ORGANIZATION". On the right, there are links for "Contact us", "Sign Out", and "English" with a dropdown arrow. A red dashed box highlights the "Sign Out" link, and a red arrow points down to it from above. Below the main navigation bar, there is a secondary navigation bar with links for "Home", "IP Services", "WIPO CASE", and "Search". Below that, there is a row of links: "Preferences", "Users Notifications", "Notifications", "Data Coverage Statistics", "User Guide", and "About". The main content area below the navigation bars is white and contains the text "WIPO CASE" in a large, bold, black font.

WIPO  
WORLD INTELLECTUAL PROPERTY ORGANIZATION

Contact us | Sign Out | English ▾

Home | IP Services | WIPO CASE | Search

Preferences | Users Notifications | Notifications | Data Coverage Statistics | User Guide | About

## WIPO CASE

# Exercise 1

- Repeat page 33 (Sign in) – 54 (Close Tab) by yourselves.

**Note: Please DON'T sign out.**



# Viewing Document List of Another Patent Family Applications

MY2011006367 x

US13378329 x JP2012518114 x

Document List

Document Name	Date	Pages/Size	
Issue Notification	2014-08-13	1p	PDF
Issue Fee Payment (PTO-85B)	2014-07-17	2p	PDF
EFS Acknowledgment Receipt	2014-07-17	2p	PDF
Fee Worksheet (SB06)	2014-07-17	2p	PDF
Notice of Allowance and Fees Due (PTOL-85)	2014-07-16	7p	PDF
Non Patent Literature	2014-07-16	6p	PDF
List of references cited by examiner	2014-07-16	1p	PDF

View 1 - 113 of 113

Biographic Data

Citation Data

Document List (US)

Time Line Tabular View Family Citations Discussion

View Application Subscribe Family Subscribe Update Indicators

BRPI1012658

SG2011097052

MY2011006367

IL216939

JP2012518114

OPERTY

# Translation

The screenshot displays a patent database interface with a document list on the left and a detailed view of a translated document on the right. Three callout boxes are overlaid on the interface:

- Translated (English)**: Points to the 'Written Amendment (TRANSLATED)' entry in the document list.
- Original (National Language)**: Points to the 'Written Amendment (ORIGINAL)' entry in the document list.
- Translated Document**: Points to the detailed view of the translated document.

**Document List (Left Panel):**

Document Name	Date	Actions
Decision to Grant a Patent (TR...	2014-08-20	[Download] [Print] [View]
Decision to Grant a Patent (OR...	2014-08-20	[Download] [Print] [View]
Written Argument (TRANSLATED)	2014-08-20	[Download] [Print] [View]
Written Argument (ORIGINAL)	2014-08-20	[Download] [Print] [View]
Written Amendment (TRANSLATED)	2014-08-20	[Download] [Print] [View]
Written Amendment (ORIGINAL)	2014-08-20	[Download] [Print] [View]
Notification of Reasons for Ref...		[Download] [Print] [View]
Notification of Reaso...		[Download] [Print] [View]
Assessment on Sea...		[Download] [Print] [View]
Assessment on Sea...		[Download] [Print] [View]
Search Report by Registered S...	2014-05-13	[Download] [Print] [View]
Search Report by Registered S...	2014-05-13	[Download] [Print] [View]
Request for Examination (TRAI...	2013-06-07	[Download] [Print] [View]
Request for Examination (ORIC...	2013-06-07	[Download] [Print] [View]
Written Notice of Determina...		[Download] [Print] [View]

**Document: Written Amendment (TRANSLATED) (2014-08-20)**

**Disclaimer:**  
This English translation is produced by machine translation and may contain errors. The JPO, the INPIT, and those who drafted this document in the original language are not responsible for the result of the translation.

**Notes:**  
1. Untranslatable words are replaced with asterisks ("\*\*").  
2. Texts in the figures are not translated and shown as it is.

Translated: 16:03:46 JST 10/23/2017  
Dictionary: Last updated 09/23/2017 / Priority:

[Document Name]Written Amendment  
[Filing date]Heisei 26(2014) August 20  
[Recipient] Patent examiner AOKI, Shigenori

[Indication of case]  
[Application number]Patent Application No. 2012-518114  
[Person who submits written amendment]  
[Identification Number]510171966  
[Name]Morpho  
[Representative]  
[Identification Number]100082108  
[Patent Attorney]  
[Name]KANZAKI, Shin'ichiro  
[Telephone number] 03-3548-0615  
[Facsimile number] 03-3548-0616  
[Dispatch number] 275127  
[Amendment 1]  
[Document to be Amended]Description  
[Item(s) to be Amended]0012  
[Method of Amendment]Change  
[Detail of Amendment]

[0012]The 1st electronic device with which the first mode of the present invention is defined as either a device (10) or a controller (11), the above-mentioned device (10) or the above-mentioned controller (11) is the control method of the device (10) by a controller (11) based on I have the 2nd electronic device defined as another side, and I a password (pi) either -- the following /1/-- the 1st electronic device of the above.

[Mathematical formula 1]  
$$E_{x,y}(x,y) : x^3 + ax + b = y^2$$

In \*\* limited object F<sub>q</sub> (q is an integer), the step which determines point P<sub>1</sub> (X, Y) of an

# Translation (IL Examination Documents)


The screenshot displays a patent database interface with a document list on the left and a detailed view of a document on the right. A yellow callout bubble with a red border points to the document view, indicating that the text is translated using Google Translate.

**Document List**

Document Name	Date	Pages/Size	Download	PDF	View	Print
Examination report	2016-07-18	2p / 0.14 ME	Download	PDF	View	Print
Claims	2016-04-04	5p / 0.04 ME	Download	PDF	View	Print
Examination report	2016-02-01	3p / 0.07 ME	Download	PDF	View	Print
Claims	2015-11-09	5p / 0.05 ME	Download	PDF	View	Print
Examination report	2015-03-19	3p / 0.13 ME	Download	PDF	View	Print
Description	2011-12-13	17p / 0.45 ME	Download	PDF	View	Print
Claims	2011-12-13	5p / 0.13 ME	Download	PDF	View	Print
Drawings	2011-12-13	4p / 0.09 ME	Download	PDF	View	Print

**Document: Examination report (2015-03-19)**

Malay Powered by Google Translate

  
 מדינת ישראל  
 משרד המשפטים

**D . Jack . 25**

tarikh : Mengenai " Khader sembilan " yang  
 9/03/2015

nombor  
 anda : 213  
 351  
 Honor  
 einhold Cohn & Partners  
 on Street 26 A '  
 ahap askar 69710

.C. V.,

Re : **Pemberitahuan kecacatan permohonan paten No. ' 216  
 939**

Rujukan : Surat Perjanjian bertarikh  
 2015/03/04

View 1 - 8 of 8

► Bibliographic Data

► Citation Data

**Translated Document  
(Google Translate)**

# Comparison of Documents (1)

Application Number \* MY2011006367 Extended Simple e.g.: ( MYPI20000041, MYPI20000344 )

Compare Maximize Close all tabs

MY2011006367 x


US13378329 x JP2012518114 x IL216939 x

Document List

Document Name	Date	Pages/Size				
Examination report	2016-07-18	2p / 0.14 ME				
Claims	2016-04-04	5p / 0.04 ME				
Examination report	2016-02-01	3p / 0.07 ME				
Claims	2015-11-09	5p / 0.05 ME				
Examination report	2015-03-19	3p / 0.13 ME				
Description	2011-12-13	17p / 0.45 ME				
Claims	2011-12-13	5p / 0.13 ME				
Drawings	2011-12-13	4p / 0.09 ME				

Document: Examination report (2015-03-19)

Malay Powered by Google Translate

  
מדינת ישראל  
משרד המשפטים

**D . Jack . 25**

tarikh : Mengenai " Khader sembilan " yang  
9/03/2015

nombor  
anda : 213  
351  
Honor  
Reinhold Cohn & Partners  
Iron Street 26 A '  
Tahap askar 69710

A . C . V . ,

Re : **Pemberitahuan kecacatan permohonan paten No. ' 216  
939**

Rujukan : Surat Perjanjian bertarikh  
2015/03/04

View 1 - 8 of 8

► Bibliographic Data

► Citation Data

**1st – 3rd Claims**

OPERTY

# Comparison of Documents (2)

Document Comparison View

IL216939:2011-12-13\_Claims\_2015-11-09

16 216939/2

CLAIMS

1. Method of control of a device by a controller on the basis of a password (11);  
said method comprising the following steps, at the device or at the controller:  
// determining on the basis of the password (11) a value for determining  
P(X,Y) on an elliptic curve

IL216939:2011-12-13\_Claims\_2011-12-13

16

CLAIMS

- Claims vs. Office action
- 1st claims vs. 2nd claims
- 1st office action vs. 2nd office action
- Claims in Office A vs. Claims in Office B
- Office action in Office A vs. Office action in Office B
- etc.

equation:

0213351647-01

Manage List Clear And Close Close

INTELLECTUAL PROPERTY ORGANIZATION

# Comparison of Documents (3)

Document Comparison View

IL216939:2011-12-13\_Claims\_2011-12-13

10

CLAIMS

1. Method of control of a device (10) by a controller (11) on the basis of a password (9):

15 said method comprising the following steps, at the device or at the controller:

/1/ on the basis of a random value  $r_1$ , determine a point  $P(X_1, Y_1)$  on an elliptic curve, in a finite field  $F_q$ ,  $q$  being an integer, of equation (1):

$$E_{a,b}(X, Y): X^2 + aX + b = Y^3 \quad (1)$$

10 /2/ obtain first and second parameters  $k$  and  $K$ , such that  $P(X, Y) = F(k, K)$  where  $F$  is a surjective function of  $F_q \times F_q$  in  $F_q$

/3/ obtain first and second parameters in encrypted form by encryption as a function of the password, and

15 /4/ transmit said first and second encrypted parameters to the controller, in which the function  $F$  is such that, regardless of  $x$  and  $x'$  input elements of  $F_q$ ,  $F(x, x')$  is a point on the elliptic curve, and the input elements do not satisfy equation (1).

20

2. Method of control according to claim 1, in which the function  $F$  is written:

$$F(x, x') = f(x) + f_0(x')$$

where  $f_0$  is an invertible function, based on the coefficients  $a$  and  $b$  of the elliptic curve, taking an input parameter and supplying a point on the elliptic curve and

25 where  $f$  is a function generating a point on the elliptic curve as a function of a parameter;

and

in which, at step /2/, the parameters  $k$  and  $K$  are obtained according to the following steps:

- randomly generating a value of the parameter  $k$ ;

30

---

17

- calculate a value of  $f(x)$ ;

- determine a value of the parameter  $k$  according to the following equation:

$$k = \int_{F_q} (f(x, x') - f(x))$$

5

3. Method of control according to claim 2, in which the function  $F$  is written:

$$f(x) = k \cdot G$$

with  $G$  the generator of the set of points on the elliptic curve; and

10 in which a value of the parameter  $k$  is determined according to the following equation:

$$k = \int_{F_q} (f(x, x') - k \cdot G)$$

4. Method of control according to claim 2, in which the function  $F$  is written:

$$f(x) = f_0(x)$$

and

in which a value of the parameter  $k$  is determined according to the following equation:

$$k = \int_{F_q} (f(x, x') - f_0(x'))$$

15

4. Method of control according to claim 2, in which the function  $F$  comprises at least one invertible function  $f_0$ , obtained by means of polynomials  $X_0(x)$ ,  $X_1(x)$ ,  $X_2(x)$  and  $U(x)$  satisfying Skhalik's equation:

$$f(x) = f_0(x)$$

IL216939:2011-12-13\_Claims\_2015-11-09

16

CLAIMS

1. Method of control of a device by a controller on the basis of a password (9): said method comprising the following steps, at the device or at the controller:

11 determining on the basis of a random value  $r_1$ , determine a point  $P(X_1, Y_1)$  on an elliptic curve, in a finite field  $F_q$ ,  $q$  being an integer, of equation (1):

$$E_{a,b}(X, Y): X^2 + aX + b = Y^3$$

12 obtaining obtain first and second parameters  $k$  and  $K$ , such that  $P(X, Y) = F(k, K)$  where  $F$  is a surjective function of  $F_q \times F_q$  in  $F_q$

13 encrypting the first and second parameters as a function of the password to obtain encrypted first and second parameters; and

14 transmitting said encrypted first and second parameters to the controller, in which the function  $F$  is such that, regardless of  $x$  and  $x'$  input elements of  $F_q$ ,  $F(x, x')$  is a point on the elliptic curve, and the input elements do not satisfy equation (1).

2. Method of control according to claim 1, in which the function  $F$  is written:

$$F(x, x') = f(x) + f_0(x')$$

where  $f_0$  is an invertible function, based on the coefficients  $a$  and  $b$  of the elliptic curve, taking an input parameter and supplying a point on the elliptic curve and

where  $f$  is a function generating a point on the elliptic curve as a function of a parameter;

and

in which, at step /2/, the parameters  $k$  and  $K$  are obtained according to the following steps:

- randomly generating a value of the parameter  $k$ ;
- calculating a value of  $f(x)$ ;
- determining a value of the parameter  $k$  according to the following equation:

$$k = \int_{F_q} (f(x, x') - f(x))$$

021331947-01

---

17

$$k = \int_{F_q} (f(x, x') - f(x))$$

3. Method of control according to claim 2, in which the function  $F$  is written:

$$f(x) = k \cdot G$$

with  $G$  the generator of the set of points on the elliptic curve; and

in which a value of the parameter  $k$  is determined according to the following equation:

$$k = \int_{F_q} (f(x, x') - k \cdot G)$$

4. Method of control according to claim 2, in which the function  $F$  is written:

$$f(x) = f_0(x)$$

and

in which a value of the parameter  $k$  is determined according to the following equation:

$$k = \int_{F_q} (f(x, x') - f_0(x'))$$

5. Method of control according to Claim 1, in which the function  $F$  comprises at least one invertible function  $f_0$ , obtained by means of polynomials  $X_0(x)$ ,  $X_1(x)$ ,  $X_2(x)$  and  $U(x)$  satisfying Skhalik's equation:

$$f(x) = f_0(x)$$

021331947-02

IL216939:2011-12-13\_Claims\_2016-04-04

16

CLAIMS:

1. Method of control of a device by a controller on the basis of a password; said method comprising the following steps, at the device or at the controller:

11 determining on the basis of a random value  $r_1$ , a point  $P(X, Y)$  on an elliptic curve, in a finite field  $F_q$ ,  $q$  being an integer, of equation (1):

$$E_{a,b}(X, Y): X^2 + aX + b = Y^3$$

12 obtaining first and second parameters  $k$  and  $K$ , such that  $P(X, Y) = F(k, K)$  where  $F$  is a surjective function of  $F_q \times F_q$  in  $F_q$

13 encrypting the first and second parameters as a function of the password to obtain encrypted first and second parameters; and

14 transmitting said encrypted first and second parameters to the controller; in which the function  $F$  is such that, regardless of  $x$  and  $x'$  input elements of  $F_q$ ,  $F(x, x')$  is a point on the elliptic curve, and the input elements do not satisfy equation (1).

2. Method of control according to claim 1, in which the function  $F$  is written:

$$F(x, x') = f(x) + f_0(x')$$

where  $f_0$  is an invertible function, based on the coefficients  $a$  and  $b$  of the elliptic curve, taking an input parameter and supplying a point on the elliptic curve and where  $f$  is a function generating a point on the elliptic curve as a function of a parameter;

and in which, at step /2/, the parameters  $k$  and  $K$  are obtained according to the following steps:

- randomly generating a value of the parameter  $k$ ;
- calculating a value of  $f(x)$ ;
- determining a value of the parameter  $k$  according to the following equation:

$$k = \int_{F_q} (f(x, x') - f(x))$$

3. Method of control according to claim 2, in which the function  $F$  is written:

$$f(x) = k \cdot G$$

021331947-02

---

17

with  $G$  the generator of the set of points on the elliptic curve; and

in which a value of the parameter  $k$  is determined according to the following equation:

$$k = \int_{F_q} (f(x, x') - k \cdot G)$$

4. Method of control according to claim 2, in which the function  $F$  is written:

$$f(x) = f_0(x)$$

and

in which a value of the parameter  $k$  is determined according to the following equation:

$$k = \int_{F_q} (f(x, x') - f_0(x'))$$

5. Method of control according to Claim 1, in which the function  $F$  comprises at least one invertible function  $f_0$ , obtained by means of polynomials  $X_0(x)$ ,  $X_1(x)$ ,  $X_2(x)$  and  $U(x)$  satisfying Skhalik's equation:

$$f(x) = f_0(x)$$

Manage List

Clear And Close

Close

# Tabular View

MY2011006367 x

Time Line **Tabular View** Family Citations Discussion

Application/Priority #	Filing/National Entry Date	Publications
<a href="#">EP2010745354</a>	2010-06-28	EP 2449721.A1.2012-05-09
FR0954473	2009-06-30	
<b><a href="#">MY2011006367</a></b>	2010-06-28	MY PI 2011006367.A.2010-12-30
FR0954473	2009-06-30	
<a href="#">CN201080039557.6</a>	2010-06-28	CN 102484589.A.2012-05-30
FR0954473	2009-06-30	
<a href="#">CA2765787</a>	2010-06-28	CA 2765787.A1.2011-01-06
FR0954473	2009-06-30	
<a href="#">US13/378,329</a>	2010-06-28	US 20120134493.B2.2012-05-31
FR0954473	2009-06-30	
<a href="#">RU201210299108</a>	2010-06-28	RU 0002533087.C2.2014-11-20 , RU 2012102991.A.2013-08-27
FR0954473	2009-06-30	
<a href="#">JP2012518114</a>	2010-06-28	JP 2012531634.A.2012-12-10
FR0954473	2009-06-30	
<a href="#">AU2010267876</a>	2010-06-28	AU 2010267876.B2.2016-02-11 , AU 2010267876.A1.2012-01-19
FR0954473	2009-06-30	
<a href="#">BRPI1012658</a>	2010-06-28	BR PI1012658.A2.2016-04-05
FR0954473	2009-06-30	

View 1 - 24 of 24

**Tabular View  
(Patent Family)**

# Family Citations

MY2011006367

Time Line Tabular View Family Citations Discussion

Citation	Category	Calim-Ref	Status	Application
<input type="checkbox"/> <a href="http://events.iaik.tugraz.at/RFIDSec08/Papers/Pub...more">http://events.iaik.tugraz.at/RFIDSec08/Papers/Pub...more</a>				CN20108003955757
<input type="checkbox"/> <a href="http://eprint.iacr.org/2009/226.pdf">http://eprint.iacr.org/2009/226.pdf</a> THOMAS ICART...more				CN20108003955757
<input type="checkbox"/> <a href="http://eprint.iacc.org/2001/098.pdf">http://eprint.iacc.org/2001/098.pdf</a> Paulo S.L.M...more				CN20108003955757
<input type="checkbox"/> PATENTSCOPE <a href="#">US2003235300</a> A (DOCDB)				JP2012518114
<input type="checkbox"/> PATENTSCOPE <a href="#">US7062044</a> B (DOCDB) 2				JP2012518114
<input type="checkbox"/> PATENTSCOPE <a href="#">US6212279</a> B (DOCDB) 2				JP2012518114
<input type="checkbox"/> PATENTSCOPE <a href="#">JP2010164796</a>				JP2012518114
<input type="checkbox"/> Eric Brier, Jean-Sebastien Coron, Thomas Icart, Da...more				JP2012518114
<input type="checkbox"/> PATENTSCOPE <a href="#">WQ2010/081980</a>				JP2012518114
<input type="checkbox"/> Thomas Icart, "How to Hash into Elliptic Curves", ...more				JP2012518114
<input type="checkbox"/> Maciej Ulas, "Rational points on certain hyperelli...more				JP2012518114
<input type="checkbox"/> PATENTSCOPE <a href="#">US6243467</a> B1				US13/378,329
<input type="checkbox"/> PATENTSCOPE <a href="#">US7062044</a> B1 2				US13/378,329
<input type="checkbox"/> PATENTSCOPE <a href="#">US7062043</a> B1				US13/378,329
<input type="checkbox"/> PATENTSCOPE <a href="#">US20030235300</a> A1				US13/378,329
<input type="checkbox"/> PATENTSCOPE <a href="#">US6212279</a> B1 2				US13/378,329
<input type="checkbox"/> PATENTSCOPE <a href="#">US20080226083</a> A1				US13/378,329
<input type="checkbox"/> PATENTSCOPE <a href="#">US7970134</a> B1				US13/378,329
<input type="checkbox"/> PATENTSCOPE <a href="#">US20040119614</a> A1				US13/378,329

Copy View 1 - 19 of 19

Currently Available for AU, CN, EP, GB, JP, KR, US



# Notification

Notification

subscribe or unsubscribe to receive notification(s) for the below selected document(s) categorise added in IL216939?

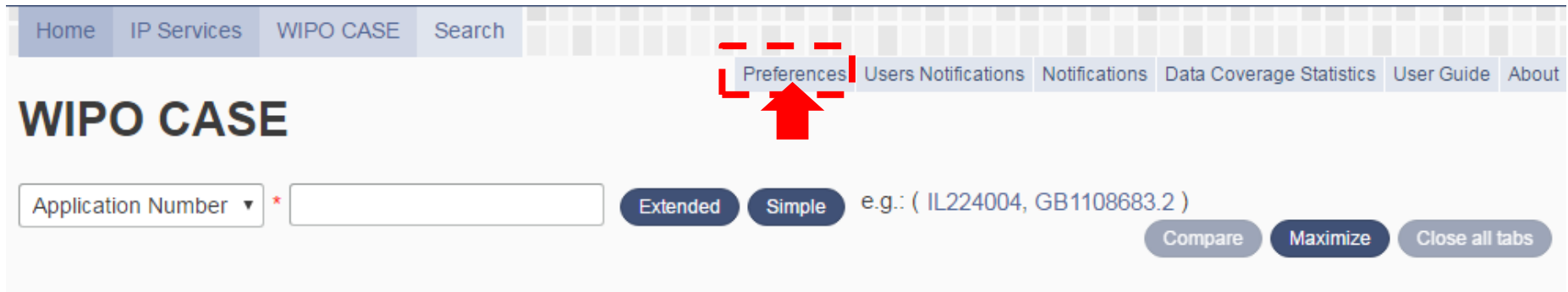
Select Categories: \*

- Specifications and Incoming Documents
- Outgoing Documents (Office actions)
- Other
- All

Yes No

Currently Available for AU, CA, GB and IL

# User Preferences



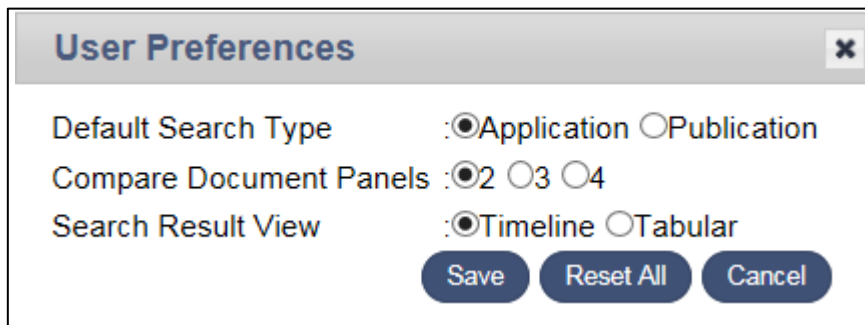
Home IP Services WIPO CASE Search

Preferences Users Notifications Notifications Data Coverage Statistics User Guide About

## WIPO CASE

Application Number ▾ \*  Extended Simple e.g.: ( IL224004, GB1108683.2 )

Compare Maximize Close all tabs



**User Preferences** ✕

Default Search Type :  Application  Publication

Compare Document Panels :  2  3  4

Search Result View :  Timeline  Tabular

Save Reset All Cancel

**Users can set up  
their preferences**

# User Guide

WIPO CASE 3.0 – User Guide, Revision 2.3  
page 9

Home

## To perform a search

1. Log on to the web portal with appropriate credentials, and then the following search window appears.

2. Select "Application Number" or "Publication Number" from Search Type drop-down list.
3. If you select "Application Number", enter the two-letter country code and the filing number without space characters in the adjacent text box. If you select "Publication Number", then enter the two-letter country code and the
4. When you enter the two letters, the country code will be shown next to the "S
5. Click the button "Extended" enter key without clicking a

## Extended Family (Time

When selecting "Extended" search, priority claims or PCT national ph

1. Fill out an application or pub
2. "Time Line" shows the res

When applications have the numbers are aligned on the

### Quick info popup

1. Put a mouse pointer onto application numbers, and "Quick info popup" is displayed.
2. "Quick info popup" shows the filing date, priorities, PCT information and the availability of search/Examination results.



DATE: SEPTEMBER 1, 2017

Data Coverage Statistics User Guide About



683.2)

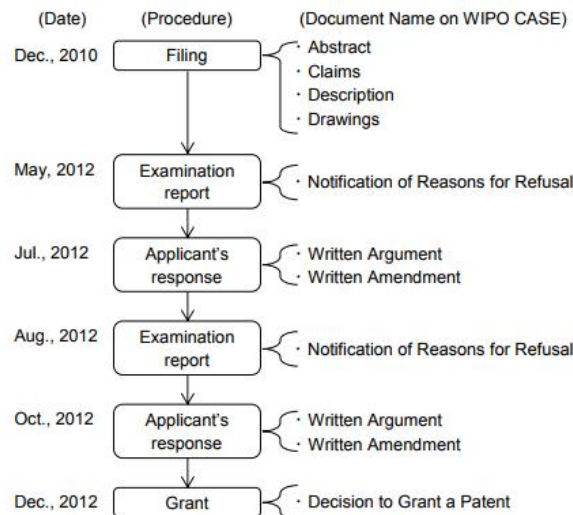
Compare

Maximize

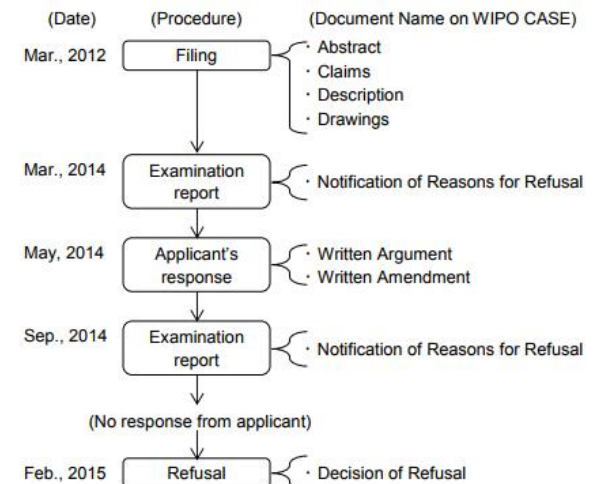
Close all tabs

WIPO CASE 3.0 – User Guide, Revision 2.3  
page 36

(Example 7-1) JP2010276000



(Example 7-2) JP2012050000



with EP data, discussion feature and some upgrades of

WIPO  
WORLD  
INTELLECTUAL PROPERTY  
ORGANIZATION

# Contact Form

WIPO  
WORLD INTELLECTUAL PROPERTY ORGANIZATION

Home › Inside WIPO › Contact Us

## Contact Us

For best results, please complete this form in Chrome, Firefox or Safari.

Topic: Patents

Sub-topic: WIPO CASE

Question:

First name (optional):

Last name (optional):

Company/Organization (optional):

Phone number (optional):

E-mail address:

Verification:  I'm not a robot

reCAPTCHA  
Privacy - Terms

If you cannot tick the verification box, please ensure you are using Chrome, Firefox or Safari. In Internet Explorer the box may not function correctly.

WIPO  
WORLD INTELLECTUAL PROPERTY ORGANIZATION

# Tips

- If patent family information hasn't been registered yet, ...

Application number: MY2014999999  
PCT application number: PCT/EP2013/000083  
Priority application number: EP2012360005

Note: This application is imaginary.

**Patent family info hasn't  
been registered yet**

National phase entry  
application

MY2014999999

Priority application

EP2012360005

PCT application

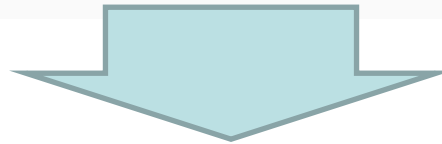
PCT/EP2013/000083



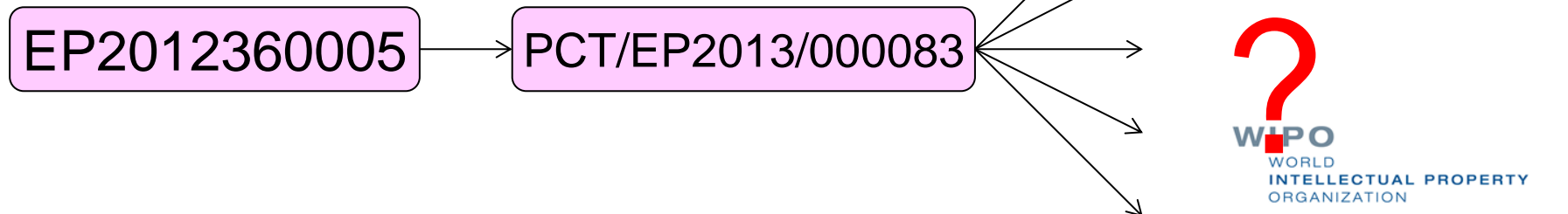
# Tips

- If patent family information hasn't been registered yet, ...

The screenshot shows the WIPO CASE search interface. At the top, there is a navigation bar with links: Home, IP Services, WIPO, Services, Users Notifications, Notifications, Data Coverage Statistics, User Guide, and About. Below this, the text 'WIPO CASE' is visible. A large yellow speech bubble with a red border contains the text 'Not Found'. Below the speech bubble, there is a red alert box that says 'Alert: Application Number not found. !'. Underneath the alert, there is a search input field with a dropdown menu set to 'Application Number' and a search button. The search input contains the text 'MY2014999999'. To the right of the search input, there are two buttons: 'Extended' and 'Simple'. Further right, there is a text field containing 'e.g.: ( MYPI20000041, MYPI20000344 )'. At the bottom right of the search area, there are three buttons: 'Compare', 'Maximize', and 'Close all tabs'.



- You can use
  - ✓ PCT application number
  - ✓ Priority application number.



# Tips

Application Number ▾ **PCT/EP2013/000083** Extended Simple e.g.: ( PCT/JP2013/081486, PCT/US2013/071150 ) Compare Maximize Close all tabs

**PCT application number**

Time Line Tabular View Family Citations Dis... Indicators

EP2012360005 CN201380006970.6 PCT/EP2013/000083 US14/374,801 JP2014553657 KR1020147020711

2011 2012 2013 2014 2015

**found**

EP2012360005

PCT/EP2013/000083

MY2014999999

CN201380006970.6

JP2014553657

KR1020147020711

WIPO

US14/374801

## Exercise 2

■ You are examining “MY2013002124” (application number).

**(1) Search for the patent family applications.**

**(2) View the following documents;**

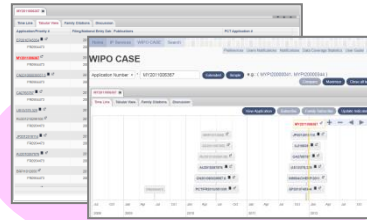
- “International Search Report” (Jun. 28, 2012) of PCT family application
- “EXAM CORRO” (Jan. 28, 2015) of AU family application
- “Notification of Reasons for Refusal (TRANSLATED)” (Sep. 2, 2014) of JP family application



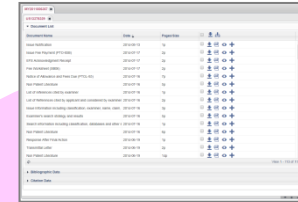
# WIPO CASE Service



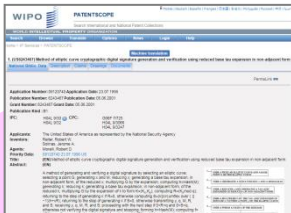
Notification



Patent family search

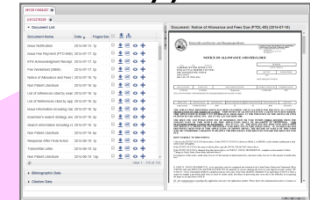


Document List  
(Prosecution history)

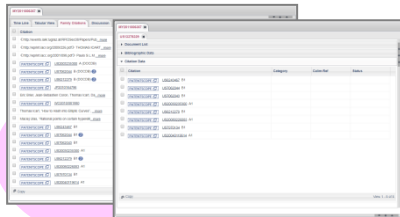


Patent document  
& translation

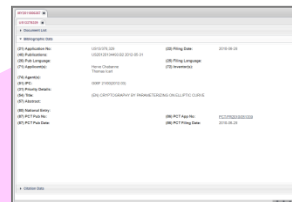
Improve  
**Efficiency** and **Quality**  
of Examination



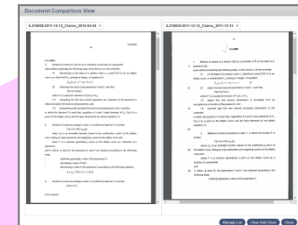
File wrapper document  
& translation



Citation Information



Bibliographic Information



Document comparison

# Outline

- Background
- WIPO CASE Service
- Functions of WIPO CASE
- **Future Development**

# Future Development of WIPO CASE

## ■ Membership

- Call for joining WIPO CASE through various opportunities
- Assist offices to take advantages of work sharing

## ■ Data scope and quality management

- Expand data scope of dossier information and patent family
- Facilitate data exchange and load process (WIPO Publish system)
- Manage data quality check system

## ■ Enhancement of service

- Improve speed performance, UI and authentication process
- Expand public service of WIPO CASE through PATENTSCOPE

## ■ Supporting activity

- Continue national workshops and regional conferences

# Thank you!