Korea Digital Signature and Future

2017. 5. 15.

한 호 현

Digital Signature

State	
Antigua and Barbuda	2006
Barbados	2001
Bhutan	2006
Cabo Verde	2003
China	2004
Colombia	
Costa Rica	
Gambia	
Ghana	
Grenada	2008
Guatemala	2008
Honduras	2013
India	2009
Jamaica	2006
Madagascar	2014
Mexico	2003
Nicaragua	2010
Oman	2008
Paraguay	2010
Qatar	2010
Rwanda	2010
nd Nevis	
the Grenadines	
Thailand	
Trinidad and Tobago	
United Arab Emirates	2006
United Kingdom of Great Britain and Northern Ireland	
Montserrat	2009
Viet Nam	2005
Zambia	2009

1999

ACTIVEX

2002

Domestic Version

Galapagos Regulation

공인인증서, 공인전자서명, PKI

- 일반적으로 알려진 공인인증서는 공인인증기관이 발급하는 인증서로 일종의 전자적 정보를 말하는데 공인전자서명의 중요한 증표로 활용된다.
- **공인인증서를 PKI나 공인전자서명으로 통칭하여 부르는 경향이 있는데 이는 잘못된 표현**이다.

공인인증서, 공인전자서명, PKI

<표 1> 중국 비은행계 공인인증서 사용 제도

第二十四条 支付机构应根据交易验证方式的安全级别，按照下列要求对个人客户使用支付账户余额付款的交易进行限额管理：
（一）支付机构采用包括数字证书或电子签名在内的两类（含）以上有效要素进行验证的交易，单日累计限额由支付机构与客户通过协议自主约定；
（二）支付机构采用不包括数字证书、电子签名在内的两类（含）以上有效要素进行验证的交易，单个客户所有支付账户单日累计金额应不超过**5000元**（不包括支付账户向客户本人同名银行账户转账）；
（三）支付机构采用不足两类有效要素进行验证的交易，单个客户所有支付账户单日累计金额应不超过**1000元**（不包括支付账户向客户本人同名银行账户转账），且支付机构应当承诺无条件全额承担此类交易的风险损失赔付责任

<표 2> 전자서명법의 공인인증서, 공인전자서명

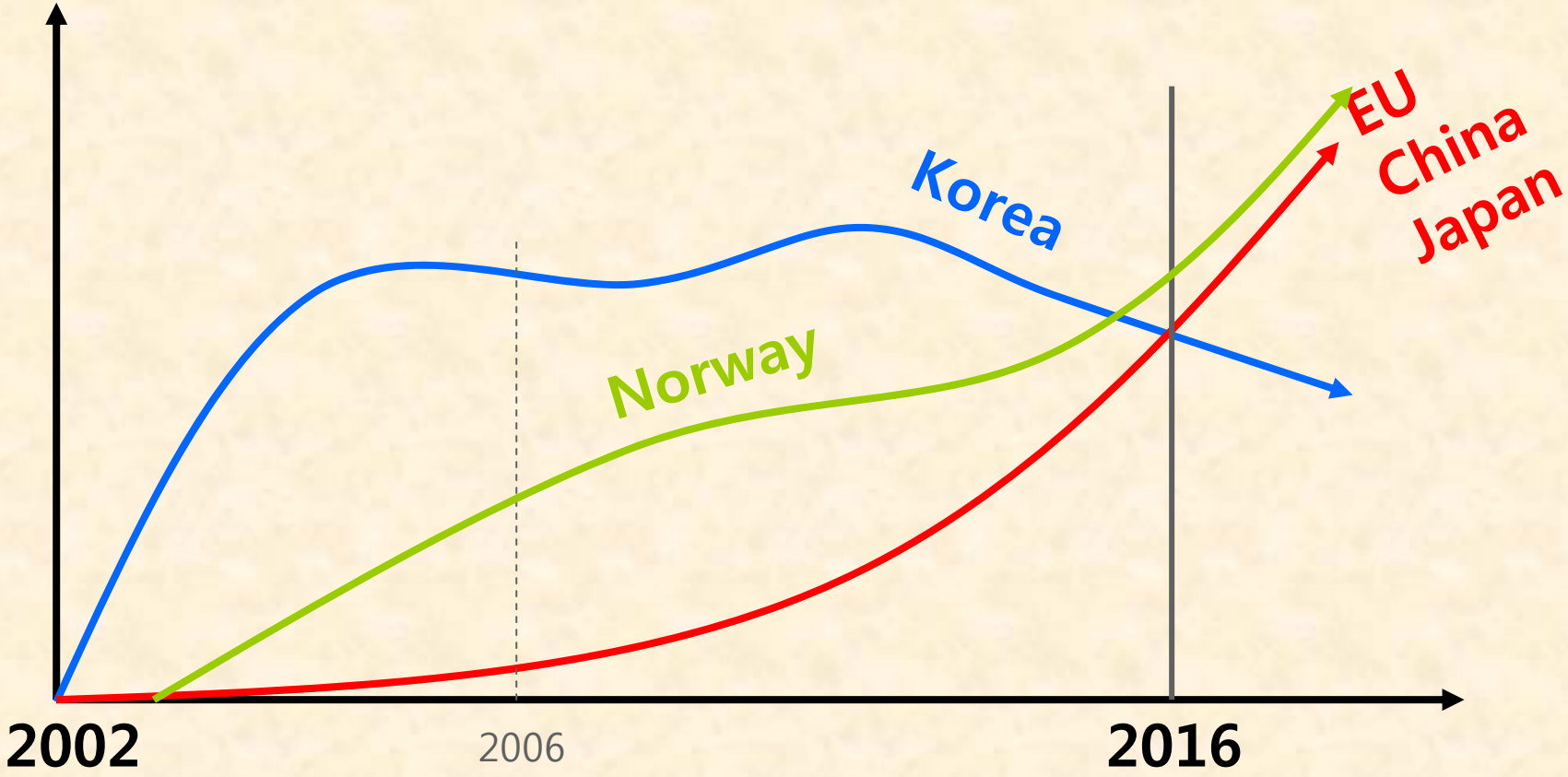
2. "**전자서명**"이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.
3. "**공인전자서명**"이라 함은 다음 각목의 요건을 갖추고 **공인인증서에 기초한 전자서명**을 말한다.
   가. 전자서명생성정보가 가입자에게 유일하게 속할 것
   나. 서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것
   다. 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것
   라. 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것
7. "인증서"라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.
8. "**공인인증서**"라 함은 제15조의 규정에 따라 공인인증기관이 발급하는 인증서를 말한다.

전자서명 요건

형식 요건	o 전자서명생성정보가 가입자에게 유일하게 속할 것	대면 확인
	o 서명 당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것	서비스 제공자 확인
기술 요건	o 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것 o 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것	PKI (비대칭키 암호화) 대칭키 암호화 방식 생체정보 •••

전자서명생성정보	=	전자서명검증정보
전자서명생성정보	=/=	전자서명검증정보

Trends



중국

o 중국은 **지난해 7월 1일부터** 비은행계 지급수단에 대하여 일정 규모 이상의 금액을 이체할 경우 **공인인증서 사용을 의무화 함**

- **비은행계 지급수단이라 함은 알리페이와 같은 결제 수단**을 말함
- **5,000위안 이상의 거래에 대하여는 반드시 공인인증서를 사용**하여야 함
- 1,000위안 이상의 거래에 대하여는 공인인증서나 다른 인증수단을 반드시 사용

截至2017年2月28日，有效电子认证证书持有量合计326,865,609张，本月减少6,008,926张，环比降低1.81%。其中机构证书45,919,675张，本月增加913,721张，环比增长2.03%。个人证书277,855,817张，本月减少6,920,794张，环比降低2.43%。设备证书3,090,117张，本月减少1,853张，环比降低0.06%。

2017年2月份电子认证证书数量统计表

证书类型	持有量（张）	本月新增数量（张）	环比增长率
机构证书	45,919,675	913,721	2.03%
个人证书	277,855,817	-6,920,794	-2.43%
设备证书	3,090,117	-1,853	-0.06%
合　　计	326,865,609	-6,008,926	-1.81%

EU

o EU는 **2016년 7월 1일부터 전자서명 관련법을 전면 도입**함에 따라 공공, 금융 분야에서 공인인증서(qualified certificate for electronic signature) 사용이 시작됨

- REGULATION on electronic identification and trust services for electronic transactions in the internal market

o **에스토니아는 전자주민증**을 이용하여 정부 및 각종 금융서비스에 **공인인증서를 사용**하고 있으며, 개별 금융 차원에서 점차 공인인증서를 사용하는 서비스를 늘려가고 있음

인도, 호주, 뉴질랜드

o 인도 중앙은행이 2015년 1월부터 금융거래에 있어서 'two-factor authentication'을 하게 함에 따라 **대부분 은행이 두 번째 인증용으로 공인인증서를 사용**하게 됨

- **인도 독일은행의 경우는 5,000,000루피 이상의 경우에는 반드시 공인인증서**를 사용하도록 하고 있음
- 인도 중앙은행은 2014년 5월 PKI관련 보고서를 통해 PKI 사용을 권장하기로 결정

o 2016년 12월부터 일정금액 이하(2,000루피)에 대하여는 'two-factor authentication'을 적용하지 않아도 되도록 이 제도를 개선함

o **ANZ은행의 경우도 공인인증서에 준하는 PKI체계**를 이용하여 사용자 인증에 사용

ANZ PKI

ANZ PKI uses digital certificates stored on smart cards to enable customers to authenticate their identity when accessing ANZ's online banking systems.

It is intended that future PKI implementations will allow customers to:

- transact with the Government using IdenTrust™ accredited digital certificates

미국 FRB

o 미국 FRB(Federal Reserve Banks)는 FRB의 각종 인터넷 서비스 이용에 PKI를 사용하도록 하고 있음

The Federal Reserve Banks operate a public key infrastructure (PKI) that manages digital certificates and the associated cryptographic keys of parties requiring access to Federal Reserve business applications. Digital certificates issued from the Federal Reserve Banks' Services Certification Authority enable authentication, key management, and digital signing capabilities in both client-to-server and server-to-server interactions. This document, a Certification Practice Statement (CPS) for the Federal Reserve Banks, describes the requirements for the issuance, management and usage of those certificates, including the practices to be used by the Federal Reserve Banks and the obligations of certificate users.

유럽중앙은행시스템, 단수케은행

o 영국 정부는 지난해 'Distributed Ledger Technology: beyond block chain'라는 보고서를 통해 분산장부 환경에 가장 적합한 인증 수단으로 인증서 기반의 PKI를 추진하는 방향을 제시함

o 유럽 중앙은행은 2013년 중앙은행결정을 통해 유럽중앙은행 PKI구축 필요성을 제기하고 그 시스템을 운영 중에 있음

> The increasing number of internal and external **users to ESCB services** requires advanced security services, such as strong authentication (i.e. two-factor authentication), digital signature and encryption.
>
> In this context it is understood that a new **Public Key Infrastructure (PKI)** capable of issuing all certificate types required for the ESCB should be implemented to address these requirements. This is known as the ESCB-PKI.
>
> The ESCB-PKI complements the services provided by other Certification Authorities accepted by the ESCB.

– 흥미로운 사실은 이 시스템에서 여전히 액티브X(ActiveX)를 사용한다는 점이다.

o 단수케 은행은 유럽 전역의 계열 은행 서비스에 PKI서비스로 사용자 인증을 하고 각종 금융 온라인 서비스를 하고 있음

> **PKI Service**
>
> Danske Bank Group PKI Service is a service for customers who make and manage certificates used to communicate with the bank through Web Services. Customers will be able to create, renew and revoke own certificates and fetch various information about them.

Blockchain/AML

Hiperledger Fabric 1.0

UK Government DLT

EU Digital Single Market Initiative

우리의 대응

디지털신원 및 전자서명에 관한 법률 제정 필요

[과제 1] 디지털신원체계 구축
[과제 2] Digital Signature의 다양화, 세분화 (미국, EU 등)
- o 일반전자서명(General Digital Signature)
- o 고급전자서명(Advanced Digital Signature)
- o 검인전자서명(Qualified Digital Signature)

[과제 3] 3세대 디지털신분증 도입 Key to Cyber Space
(디지털신원 + 전자서명 + 디지털화폐)
개인정보 및 관련 정보의 자기 통제권 보장 수단

문의

- howhan@khu.ac.kr