Friday, 24 April 2015

A Study of Cryptographic Algorithms Transition in the Electronic Bidding Core System

Hiroyuki Ishiwata

Electronic Bidding Core System
Development Consortium Secretariat

JACIC

Agenda

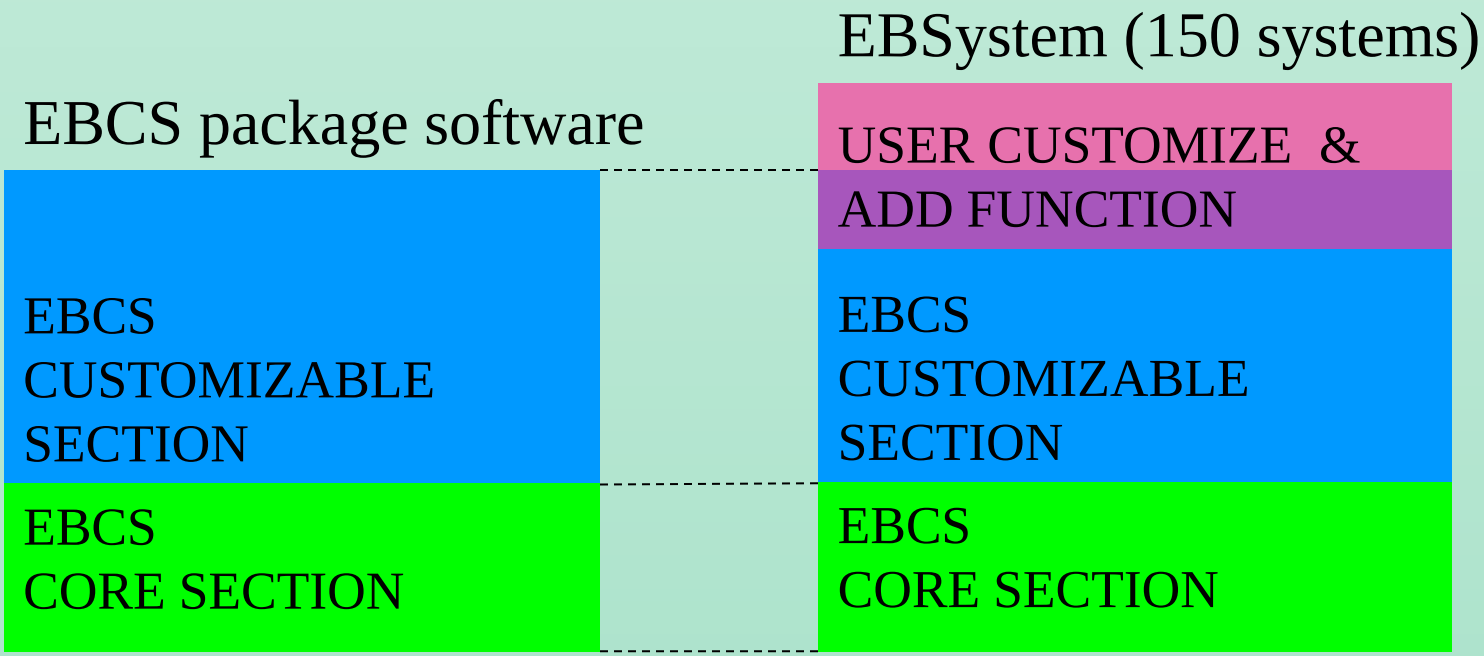
- Electronic Bidding Core System
- Cryptographic Algorithms
- Cryptographic Algorithms for Electronic Bidding Core System

Electronic Bidding Core System (EBCS)

- Package Software for building Electronic Bidding System
- JACIC and SCOPE(Service Center of Port Engineering General Incorporated Foundation) developed
- various procurement method
- series of procurement procedure
- objective

Electronic Bidding System(EBSystem)

- computer system which was built with EBCS



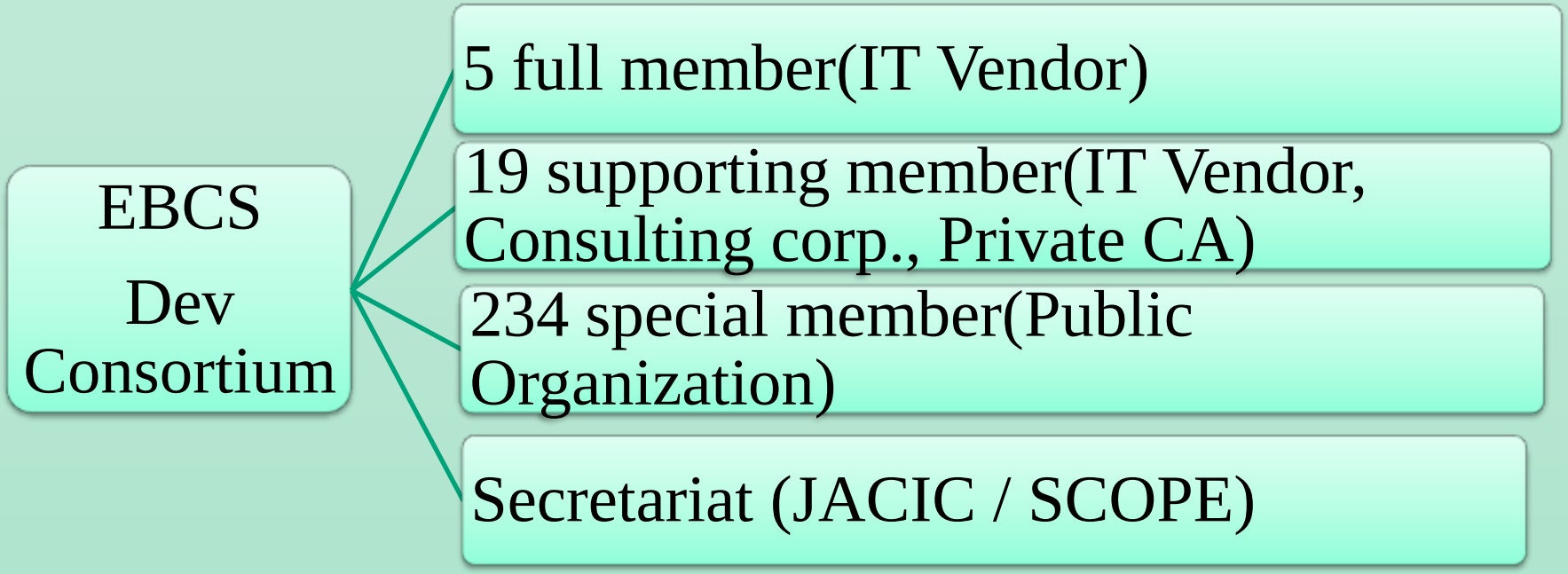
number of EBCS Users (Public Organization)

Public Organization	total
Central Ministries	8
Public Corporations and Organizations	17
Prefectures adoption rate 99 % !	46
Ordinance-Designated City	19
Municipality	570

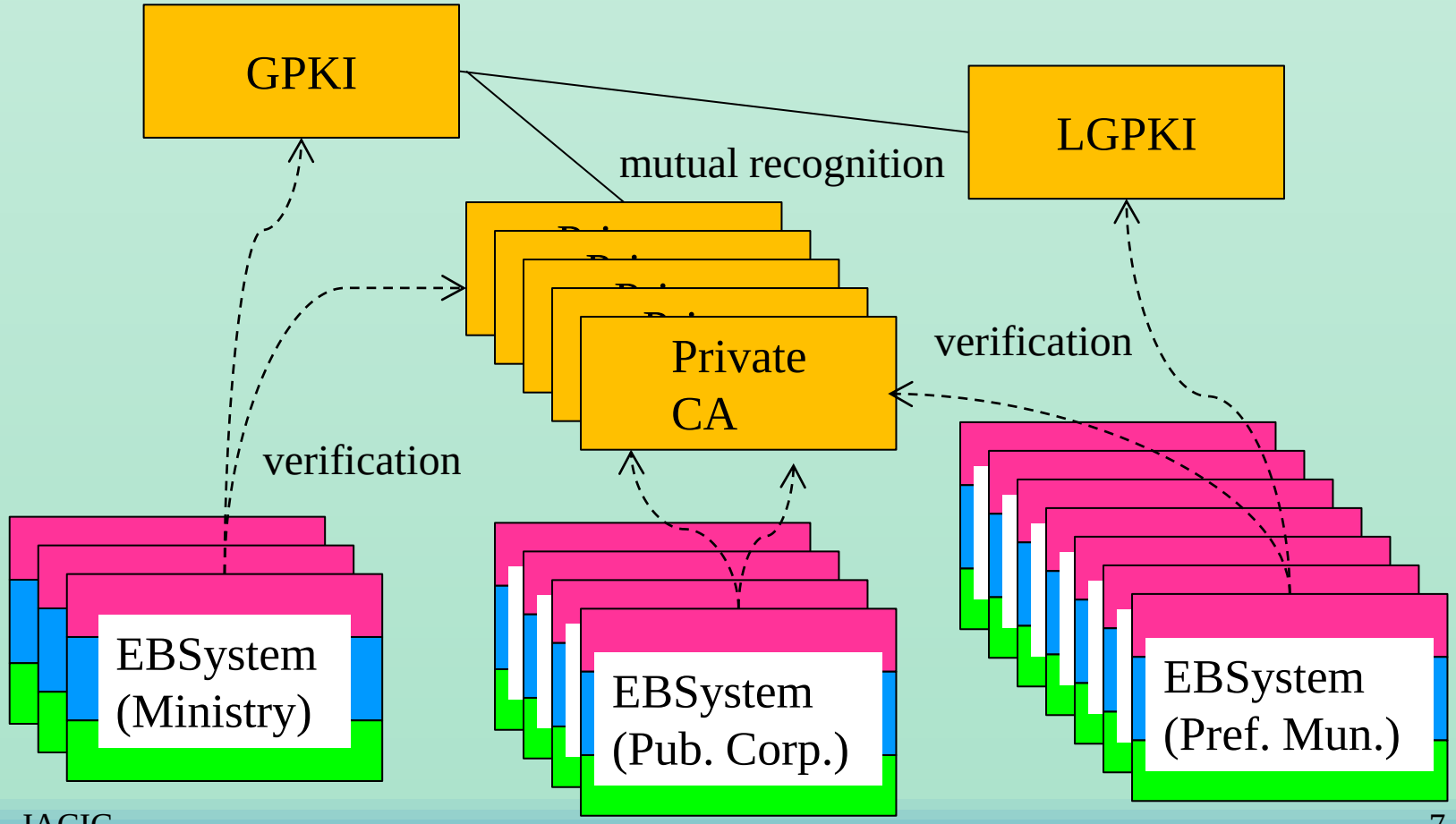
GRAND TOTAL is **660** Organizations !

EBCS Development Consortium

- Specifications study of EBCS



Authentication infrastructure of EBCS



Cryptographic algorithms in Japan

- COMPROMISE OF CRYPTOGRAPHIC ALGORITHMS

Current algorithms will be decoded in 2015.

- 2008 - 2012

Government

Sep.2014: Start of New Alg. Verification
End of 2015: End of Old Alg. Verification

- 2014

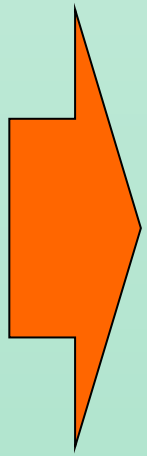
Government

Sep.2014: Alg. Transition GPKI, LGPKI
Oct.2014: Alg. Transition private CA

Cryptographic algorithms in EBCS

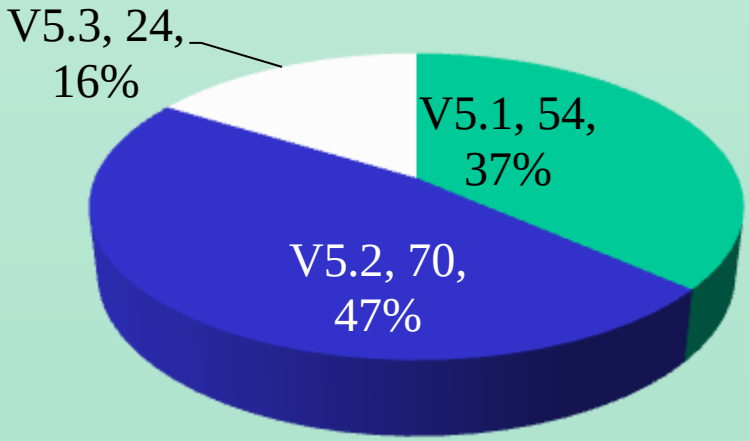
- digital government recommendation code list (CRYPTREC)

algorithm	old	new
Common key cryptosystem algorithm	3-key Triple- Data Encryption Standard(DES)	Advanced Encryption Standard (AES)
Public key cryptosystem algorithm	Rivest Shamir Adleman (RSA)1024	RSA2048
Digest algorithm	Secure Hash Algorithm(SHA)	SHA-2
Signature Algorithm	SHA1withRSA	SHA2withRSA



Transition of EBSystems

- Oct.,2014, Transition of EBSystem has been carried out
- Most of EBSystem was successfully completed!



modify 84% EBSystems!

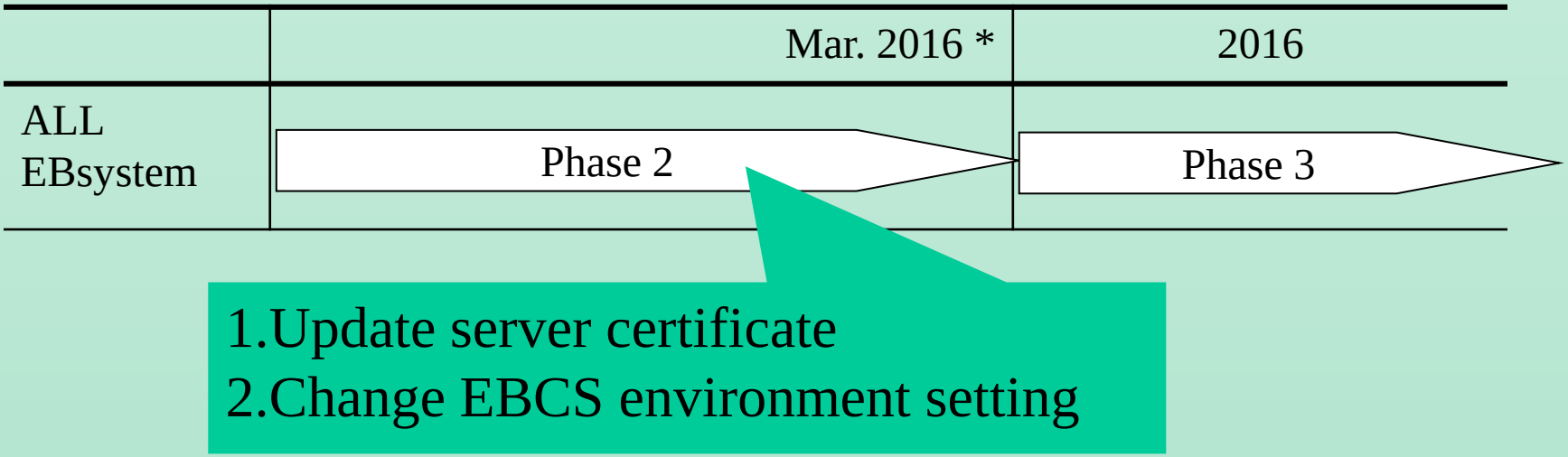
Agenda in EBCS Transition

- Technical problems and solutions
  - Possibility of system delay
  - Increase of inquiry to help desk
- Information sharing with related organizations
  - Consensus-building
  - Review

Evaluation

- Technical problems and solutions
  - did not receive the report about delay
  - number of inquiry does not increase
- Consensus-building
  - Support of GPKI, LGPKI, Private CA
  - Consortium member’s review

Conclusion



* In view of the expiration of private CA certificate , end of phase 2 seems to be postponed until 2019

Thank you for your listening.