TRANSITIONING OF CRYPTOGRAPHIC ALGORITHMS IN THE ELECTRONIC BIDDING CORE SYSTEM

2013.11.8

JACIC

Hiroyuki ISHIWATA

introduce myself

- author name: Hiroyuki ISHIWATA
- Affiliations: JACIC Systems Engineering Division, Core System Development Consortium Secretariat
- Charge duties: Specifications Study, Improvement, Maintenance, Administration of Service Center of Electronic Bidding Core System (“Core System”)

What is cryptographic algorithm?

- Technology of Electronic Authentication
- www.cryptrec.go.jp/english/index.html

CRYPTREC
Cryptography Research and Evaluation Committees

- Crisis of Code Technology

Decision of Japanese government

- April 22, 2008
  Transitioning guidelines of Japanese government
  All information systems of government have to transit to new algorithm by end of 2013
- November 1, 2012
  Start date of issue digital certificates by new cryptographic algorithm
  ⇒ early after the end of September, 2014.
  End time of current cryptographic algorithm verification
  ⇒ end of 2015.
  (but the validity period of the issued digital certificate remains, if unavoidable, end of 2019)
- http://www.nisc.go.jp/conference/seisaku/index.html

		Phase1 ～2014/9	Phase2 2014/9～	Phase3 2016 or 2019～
current algorithm (SHA-1 and RSA1024)	signature	OK	OK	-
	signature verification	OK	OK	-
new algorithm (SHA-256 and RSA 2048)	signature	-	OK	OK
	signature verification	-	OK	OK

Transition of GPKI and LGPKI

- GPKI: Government Public Key Infrastructure
  www.gpki.go.jp/
- LGPKI： Local Government Public Key Infrastructure
  www.lgpki.jp/
- in accordance with government guidelines, cryptographic algorithm transition of GPKI and LGPKI will be carried out September 2014 around

Transition of Private Certificate authority (CA)

- it would be carried out October 2014 around
- update certificate authority key (4 CA)
- new certificate authority (2 CA)

e-Probatio NTTネオメイトの電子認証サービス

JapanNet

日本電子認証株式会社

TDB電子認証サービス TypeA

TOiNX CERT

Transition of "Core System"

2009-2013	twice a year, in user conference, JACIC explained how to apply to user's systems
August, 2012	Provided transition module (beta version)
June, 2013	Provided transition module (official version)
2013-	Provide technical information by Service Center Home Page and e-mail

About “Core System”

- Purpose: Efficiency of Office, Increase Transparency, Reduction of Cost, Expansion of Bid Opportunities
- Reliability
- General versatility
- more than 550 organization users (including sharing use)
- "Core System Development Consortium"
- "Core System Service Center”
- latest version v5.3 (July, 2013 release)
- JACIC(Japan Construction Information Center) and SCOPE(Service Center of Port Engineering) developed

System Features of “Core System”

- Package Software
- Various Construction phase
- Various bid methods
- Security and authentication
- apply the latest technology
- Choice of operation method
- Benefits of bidders

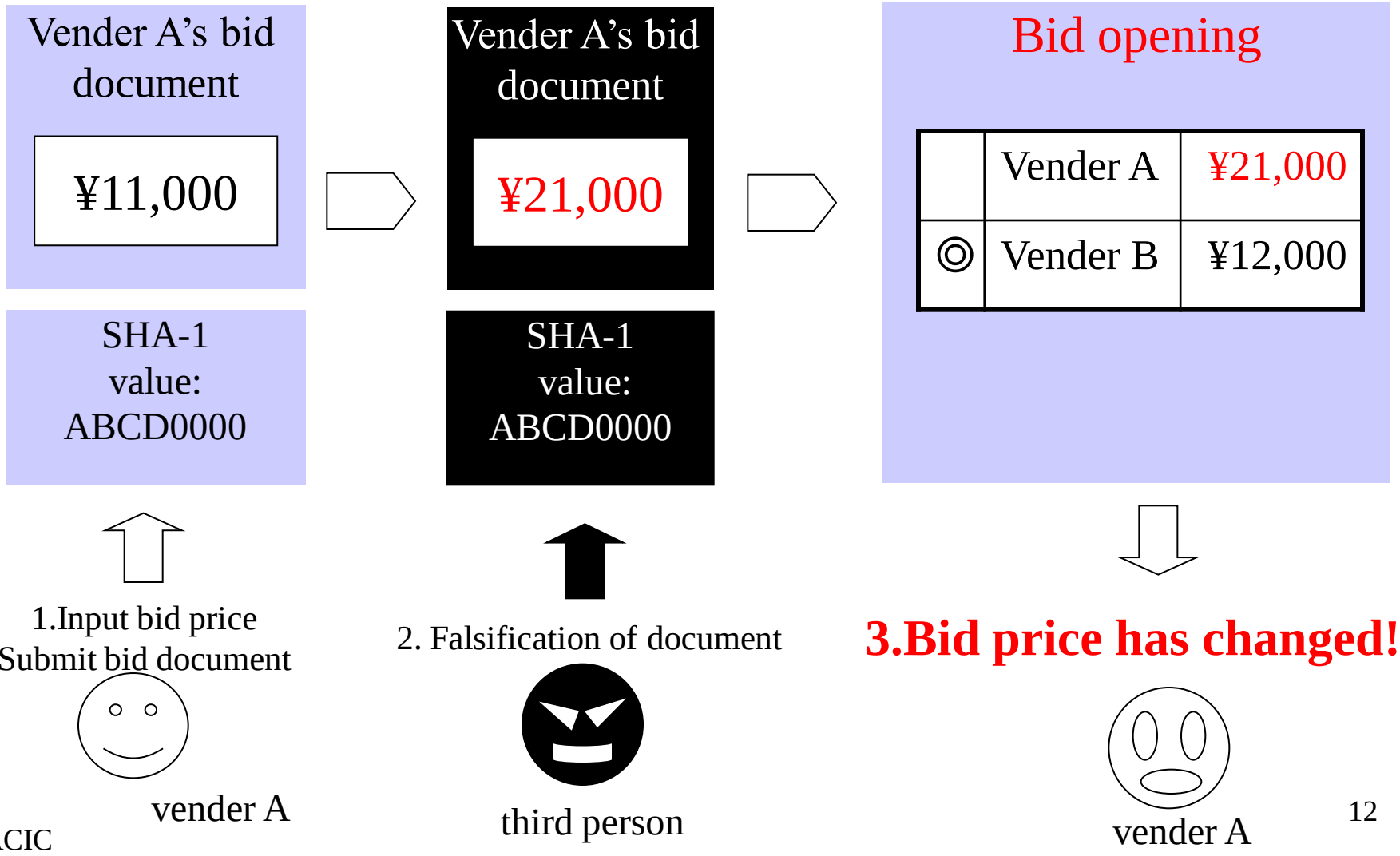
Stakeholder of “Core System”

category	Category	relations
Electronic bidding core system development consortium	Secretariat	JACIC. operate consortium
	Full member	5 vendor. participate in specification study
	Supporting member	vendor, private CA, etc.. receive results of study
	Special member	Core system user, future user.
JACIC		development, Improvement, maintenance
Certificate authority (CA)	GPKI	issue IC card for government staff
	LGPKI	issue IC card for local government staff
	private CA	issue IC card for Bidders
	RTLAB	Ministry of Justice. issue IC card for Bidders
Ordering party	national ministries Prefectures etc.	operates e-bidding system using Core System
Bidders	Construction, Civil Engineering, goods or service suppliers	Companies to participate in the bidding

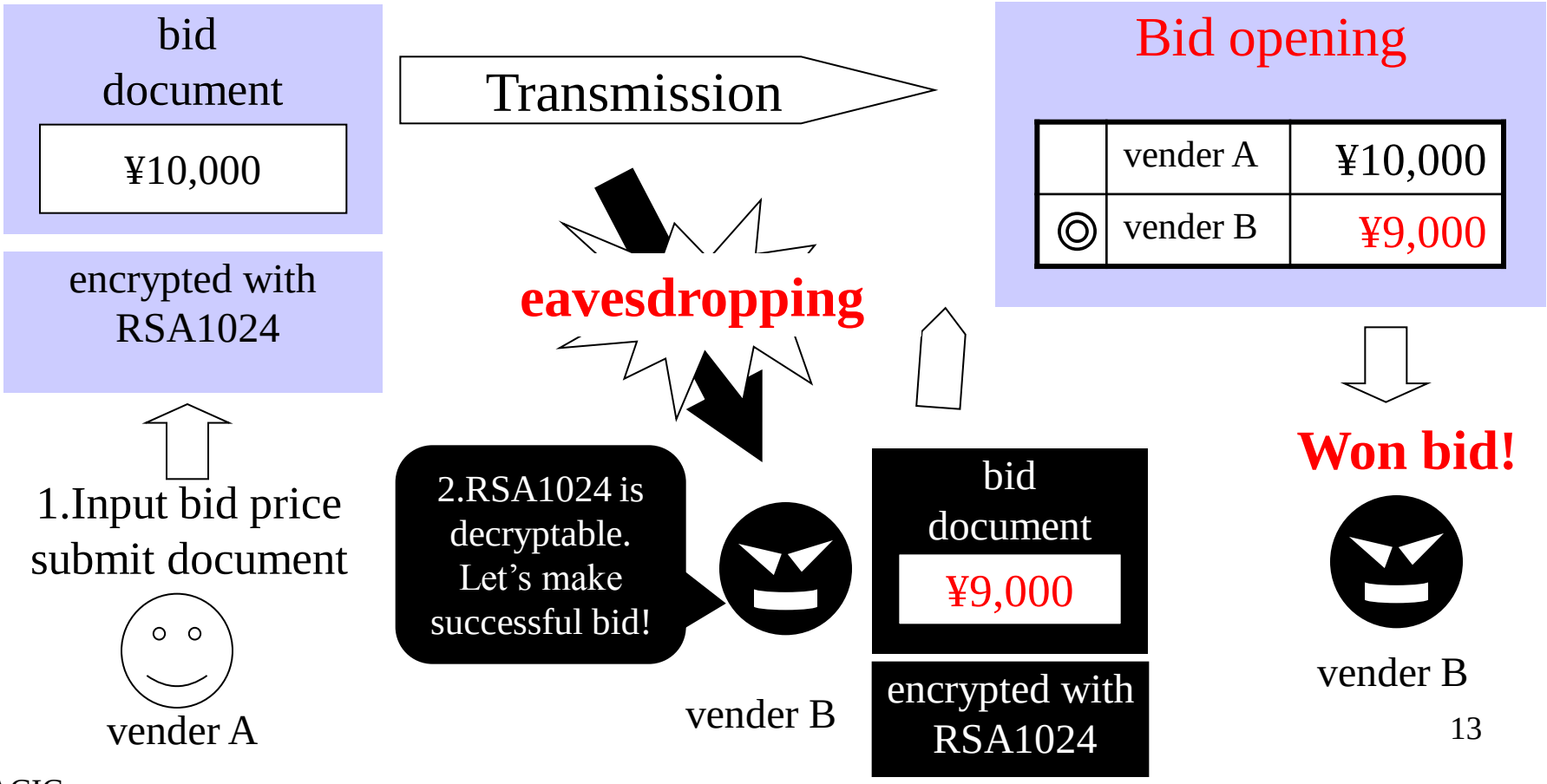
Current and new alg. of “Core System”

name	category	Point-of-use	New alg.
SHA-1	Hash Function	Certificate Validation Signature/ Signature Verification Hash Value Calculation	SHA-256
RSA1024	Public Key Cryptography	Certificate Validation Signature/ Signature Verification Encryption/ Decryption	RSA2048
3key-Triple DES	Common key Cryptography	Encryption/ Decryption	AES

impact of SHA-1 compromised (example)

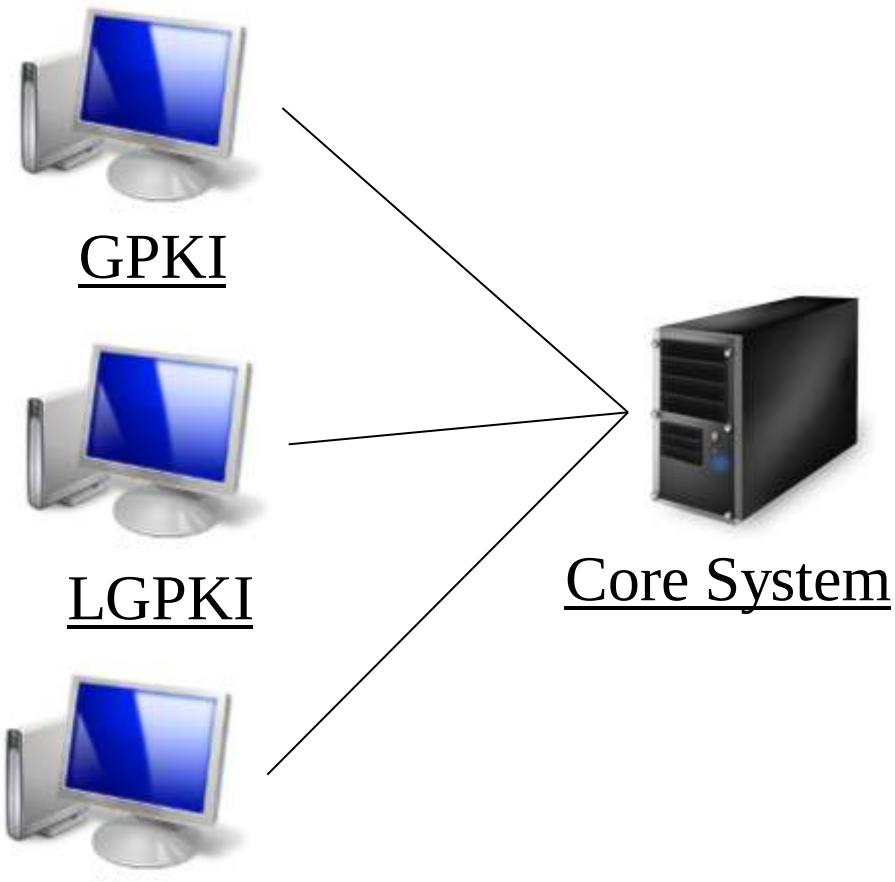


impact of RSA1024 compromised (example)



update point of “Core System”

client software (JACIC, CA, users)
Cryptographic Library (vender)
IC card reader (CA, vender)
IC card (CA)

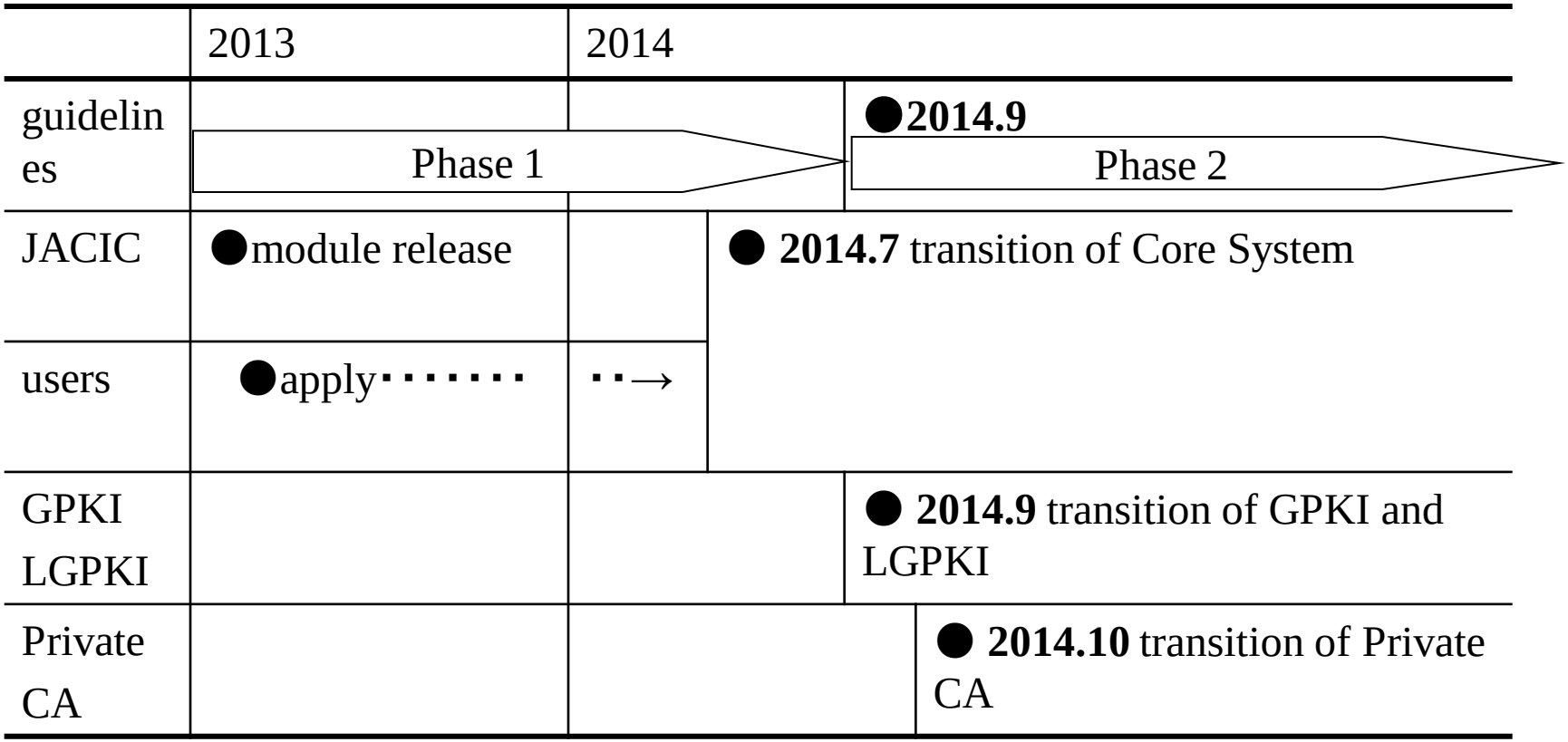


Core system customizable section (JACIC,users)
Core system core section (JACIC)
Cryptographic Library (vender)
OS middleware (vender)

Cryptographic algorithm transition specification of “Core System”

- to have a calendar inside, realize mechanism of switching Phase 2, Phase 3
- Referring to advice of IPA, changed 3key-Triple DES to AES
- In order to promote update of client software, displays warning message
- time of Signature verification, display name of algorithm on window

Schedule



Time of Phase3 is not decided. But, Core System needs only calendar setting.

User Support of JACIC

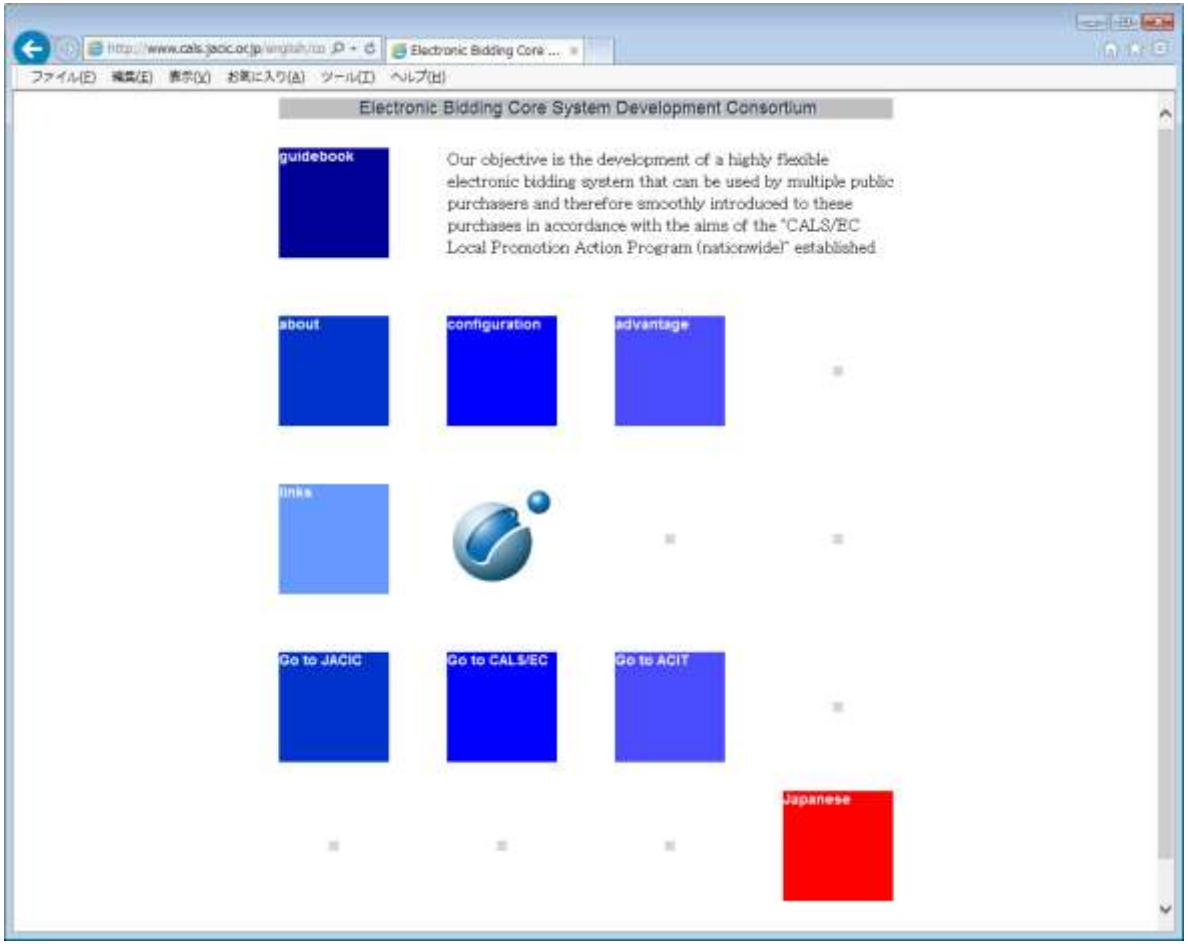
- JACIC promotes electronic bidding
- JACIC supports all public organization uses to complete cryptographic algorithm transition successfully

Future improvements

- Version / revision up support Java 7
- Supports Windows 8/8.1
- Internet Explorer 10/11
- Improvement of goods services function
- Comprehensive evaluation of business
- Performance Improvement
- Applet signature
- Spread to the municipality

Reference

- Electronic Bidding Core System Development Consortium
  - http://www.cals.jacic.or.jp/english/coreconso/



Thank you very much.