EUROSMART

The Voice of the Smart Security Industry

Cryptographic constraints for Smart Security Devices' application

June 2008

Foreword

Smart Security Industry needs to have a clear overview on the level of security required for cryptographic mechanisms in the next 'x' years. Such information is not only mandatory for the silicon vendors to anticipate hardware availability for any market request , but also to card manufacturers and all other players who are involved in the security business and want to be state of the art technology wise. However, many voices exist that are sometimes not consistent: academic, governmental institutions, private organizations…

The goal of this document is to provide an overview on the cryptographic mechanisms specified today in the main smart security devices applications to compare with the recommendation of the different governmental institutions, and to provide some recommendation to the Smart Security industry about how to move on.

1. Cryptographic robustness

Cryptographic mechanisms are tools which aim assuring confidentiality, integrity, authenticity and non-repudiation of information. These security properties are maintained along with the robustness of the cryptographic algorithm.
Due to major developments in cryptographic science and the increasing calculation capacities of computers, this robustness evolves in time. An implementation that is considered as secure today may be cracked tomorrow.
Some governmental institutions have published recommendations on cryptographic mechanisms usage, mainly in terms of algorithm to use and associated cryptographic keys length.
Sometimes it is difficult for developers to get to the right information and know what implementation is still considered as secure and for how long.

Indeed a very useful site is **http://www.keylength.com/**
This web site implements mathematical formulas and summarizes reports from well-known organizations, allowing the developer to find the appropriate key length for desired or required level of protection.

Detailed reports are available from the following governmental public websites.

- In France, DCSSI has published cryptographic recommendations for a standard robustness certification level.
  http://www.ssi.gouv.fr/fr/politique_produit/catalogue/pdf/mecanismes_cryptographique_v1_10_standard_uk.pdf
- In Germany the Federal Network agency provides recommendation for electronic signature (but in German only)
  http://www.bundesnetzagentur.de/media/archive/12198.pdf
- The BSI provides recommendation for eCard projects (mainly health cards):
  http://www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf
- In the USA, the NIST Computer Security Resource Center (CSRC) provides recommendation also for key management and hash functions
  http://csrc.nist.gov/groups/ST/toolkit/index.html
  http://csrc.nist.gov/groups/ST/hash/index.html

These documents provide an extract of rules and recommendations for implementation. Not all details are described in this document. It is recommended for users to read the originally documents. This should be checked in detail by developers before implementation.

2. Cryptographic standard used for smart cards

The table below presents the algorithms, blocks and key size used today in different standards.

Application type	Algorithms	Key length
Bank (EMV) SDA	3DES – CBC mode 3DES – ECB mode	112 bits (64 bits blocks) 112 bits (64 bits blocks)
Bank (EMV) DDA	3DES- CBC 3DES – ECB mode SHA-1 RSA	112 bits (64 bits blocks) 112 bits (64 bits blocks) 160 bits 1024 to 1984 (modulo 8)
Signature (e-Sign)	3 DES–CBC mode RSA SHA-1, RIPEMD-160 SHA-224, SHA-256, SHA-384 Diffie-Hellman (for key agreement)	112 bits (64 bits blocks) 1024 to 2048 (modulo 8) 160 224, 256, 384 _
ID cards (IAS)	3DES-CBC mode RSA SHA-1 SHA-256 Diffie-Hellman (for key agreement)	112 bits (64 bits blocks) 1024, 1536, 2048 bits 160 bits 256 bits _
e-passport BAC	3DES-CBC Retail MAC (DES) SHA-1	112 bits (64 bits blocks) 112 bits (64 bits blocks) 160 bits
e-passport EAC	3DES-CBC mode Retail MAC (DES) SHA-1 SHA-224 SHA-256 RSA Diffie-Hellman or Elliptic Curves (for key agreement)	112 bits (64 bits blocks) 112 bits (64 bits blocks) 160 bits 224 bits 256 bits 1024 to 2048 (modulo 8) _
Health	RSA SHA-1 SHA-256 3DES Retailed MAC 3TDES	1024 to 2048 (modulo 1) 160 bits 256 bits 112 bits (64 bits blocks) 168 bits
Java Card 2.2.1	3DES RSA AES RIPDEM160 SHA-1	112 bits (64 bits blocks) 1024 to 2048 bits 128,192,256 (block of 128 bits) 160 bits 160 bits

Note that future updates of standards will recommend replacing DES by AES as soon as possible

3. Governmental institutions recommendation

The following tables summarize what can be found about keys length and limitation of usage for applications to be certified by DCSSI (France), BSI/BNA (Germany) and NIST (USA)

France DCSSI: Standard level

Cryptographic Primitive	Minimum Key/Parameter Size	Expiration Date
Symmetric Keys	80 bits	2010
Symmetric Keys	100 bits	
Symmetric Encryption Block	64 bits	
RSA modulus	1536 bits	2010
RSA modulus	2048 bits	2020
RSA secret exponent	Same size as modulus	
RSA public exponent (encryption)	$2^{16}+1$	
DL over GF(p) : prime p	1536 bits	2010
DL over GF(p) : prime p	2048 bits	2020
DL over GF(2^n) : integer n	2048 bits	2020
DL : order of subgroup : prime q	160 bits	2010
DL : order of subgroup : prime q	256 bits	
ELC over GF(2^n) : integer n	prime n	
ELC : order of subgroup : prime q	160 bits	2010
ELC : order of subgroup : prime q	256 bits	
Hash function digest (SHA)	160 bits	2010
Hash function digest (SHA)	256 bits	

Germany BSI/BNA recommendation for electronic signature

Function	Algorithm	Key size in bits	Recommendation
Hash	RIPDEM160	160	<=2010
	SHA-1	160	<= 2007 <= 2009 for generation of qualified signatures <= 2014 for verification of qualified certification
	SHA- 224,SHA-256, SHA-384, SHA-512	224, 256 384, 512	<=2014 and after

Function	Algorithm	Key size in bits	Recommendation
Asymmetric	RSA	1024 1280 1536 1728 1976 2048	<=2007[1] <=2008 <=2009 <=2010 <=2014 Recommended
	DSA	p: 1024 1280 1536 2048 q: 160 224	 <=2007 <=2008 <=2009 Recommended for > 2009 <=2009 Recommended for >2009
	DSA based on groups $E(F_p)$ – EC	p: 192 q: 180 224	 <=2009 <=2009 <=2014
	DSA based on groups $E(F_{2^m})$ – EC	m: 191 q 180 224	 <=2009 <=2009 <=2014
Random number	TRNG PRNG	Class P2 hoch Class K3 with 80 bit seed (100 bit recommended) Class K4 with 100 bit seed (120 bit recommended)	>=2011 <2009 >=2010

Germany BSI recommendation for eCards (health cards)

Function	Algorithm	Key size in bits	Recommendation
Hash	SHA-1 RIPEMD-160 SHA- 224,SHA-256, SHA-384, SHA-512	 160 224, 256 384, 512	<=2007 <=2009 <=2013
Asymmetric	RSA	1024 1976 2048	<=2007 <=2013 <=2013
	DSA	p: 1024 2048 q: 160 224	 <=2007 <=2013 <=2007 <=2013
	DSA based on groups	q:	

[1] A transission period is defined until March 2008, where RSA with 1024 bit keys may be used.

Function	Algorithm	Key size in bits	Recommendation
	$E(F_p)$ – EC	160 224	<=2007 <=2013
Symmetric	2TDES 3TDES		<=2009 <=2013
	AES-128 AES-192 AES-256		<=2013
Random number	TRNG PRNG	P2 hoch K3 hoch	

NIST recommendations

Function	Algorithm	Key size in bits	Recommendation
Hash	SHA-1 SHA-224, 256, 384,512	160 224,256,384, 512	Not recommended
Symmetric crypto	2 TDEA 3 TDEA AES	80, 112, 128 128	Until 2010 Until 2030 After 2030 Highly recommended
Asymmetric crypto	RSA	1024 2048 3072	Until 2010 Until 2030 After 2030
Key agreement	DH or elliptic curves	_	
Random number generation	TRNG PRNG NRBG		True random Pseudo Random Non deterministic random bit generator

4. Conclusion

Even if all institutions do not present exactly the same results, we can see clearly the trends of recommendations
- For Symmetric types, 3DES is limited to a 64 bit block and should be replaced as soon as possible by **AES** that offers larger size blocks of 128.
- For Asymmetric types, RSA keys should go also to 2048 bit key length.
- For hash functions SHA-1 is no longer welcome, and for long term security it should be replaced at by at least SHA-224, but switching directly to SHA-256 is easier for developers.

Developers should also be careful about the standard chosen for Random Number Generation as in this area the rules are different from one government to another (AIS31, AIS20).

5. Glossary

3 DES	Triple DES
2TDES	Triple DES with key length of 128 bit
3TDES	Triple DES with key length of 192 bit
AES	Andvanced Encryption Standard
AIS	Anwendungshinweise und Interpretationen zum Schema
AIS20	Fuktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
AIS31	Fuktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
BNA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC	Cipher Block chaining
DES	Data Encryption Standard
DCSSI	Direction Central de la Sécurité des systèmes d'Information
DH	Diffie Hellman key agreement scheme
DL	Discrete algorithm
DSA	Digital Signature Algorithm
ELC	Elliptic curves
NIST	National Institute of Standards and Technology
NRBG	Non Deterministic Random Bit Generator
TRNG	True Random Number Generator
TDEA	Triple Date Encryption Algorithm (AES, 3DES)
PRNG	Pseudo Random Number Generator
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm

Eurosmart is an international non-profit association located in Brussels and representing 25 companies of the smart security industry for multi-sectors applications. Founded in 1995, the association is committed to expanding the world's smart secure devices market, developing smart security standards and continuously improving quality and security applications.

Manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers gather and work into dedicated working groups on communication and marketing, security, electronic identity and new form factors, and prospect emerging markets. Members are largely involved in political and technical initiatives as well as research and development projects at the European and international levels

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry".

More information: www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21
B-1000 Bruxelles
Tel. (+32) 2 506 88 38/ Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com