信頼される安心を、社会へ。
SECOM

2030年暗号移行問題について

2023年7月26日

松本　泰　（セコム株式会社IS研究所顧問）

2030年暗号移行問題について

- 2003年に公開された「CRYPTREC電子政府推奨暗号リスト」にみられるような客観的に評価された暗号アルゴリズム、この評価を前提に標準化されたオープンな暗号技術は、深く社会基盤に組み込まれ、それに伴いデジタル社会を大きく前進させた。
- こうした社会基盤に組み込まれた暗号アルゴリズムの最初の移行が「2010年暗号移行問題」とされた。
- 本講演では、公開鍵暗号基盤（PKI）を中心に「2010年暗号移行問題」を振り変えり、より深く社会に浸透した暗号技術に対する「2030年暗号移行問題」について考察する。
- また、デジタル社会における暗号技術の社会への浸透に伴うCRYPTRECが果たすべき役割の変化についても考察する。
- キーワード
  - 80bitセキュリティ　　RSA1024bit with SHA-1など
  - 112bitセキュリティ　　RSA 2048bit with SHA-2(SHA-256)など
  - 2010年問題　　112bit セキュリティへの移行が2010年問題
  - 120bit セキュリティ　　RSA 3072bit with SHA-2 (SHA-256)など
  - 2030年問題　　120bitセキュリティへの移行が2030年問題

- （１）　２０１０年暗号移行問題の振り返り
- （２）　欧州における2030年暗号移行問題の対応方針と状況
- （３）　まとめ

2010年暗号移行問題の振り返り

喉元過ぎれば熱さを忘れる？？

日本銀行金融研究所ディスカッション・ペーパー

暗号アルゴリズムにおける2010年問題について　宇根 正志、神田 雅透　　2005年11月

https://www.imes.boj.or.jp/research/abstracts/japanese/05-J-22.html

- 金融分野においては、金融取引に用いられる各種データの機密性や一貫性を確保する手法、あるいは、取引相手を認証する手法の要素技術として暗号アルゴリズムが活用されている。現時点では、共通鍵暗号は2-keyトリプルDESとRC4、公開鍵暗号は鍵長1024ビットのRSA、ハッシュ関数はSHA-1が主流になっているとみられている。
- しかし、これらの暗号アルゴリズムは、今後のコンピュータのコスト・パフォーマンス向上や暗号解読技術の進展等を前提とすると、今後10～15年にわたって十分な安全性を確保することが難しいとの見方が暗号研究者の間で強まっている。また、従来暗号アルゴリズムの安全性について実質的に「お墨付き」を付与してきた米国立標準技術研究所（NIST）は、より安全な次世代の暗号アルゴリズムへの移行を図るため、2-keyトリプルDESや鍵長1024ビットのRSAやSHA-1など現在主流とされている暗号アルゴリズムを2011年以降米国連邦政府機関のシステムで使用しない方針を各種ガイドラインの中で示している。
- こうしたことから、暗号アルゴリズムの移行を今後どのように進めるかが重要な問題となってきており、本稿ではこうした問題を総称して「暗号アルゴリズムにおける2010年問題」と呼ぶ。NISTが期限として定めている2010年までに移行を完了させるためには、本問題への対応について早急に検討を開始することが求められる。
- 本稿では、現在主流とされている暗号アルゴリズムの安全性評価結果について紹介したうえで、暗号アルゴリズムにおける2010年問題とその影響、NISTの対応状況等について説明する。さらに、今後金融分野において本問題に対処していくうえで留意すべき点について考察する。

移行の問題
暗号アルゴリズムの危殆化問題、移行問題

セコム IS研究所 Intelligent Systems Laboratory

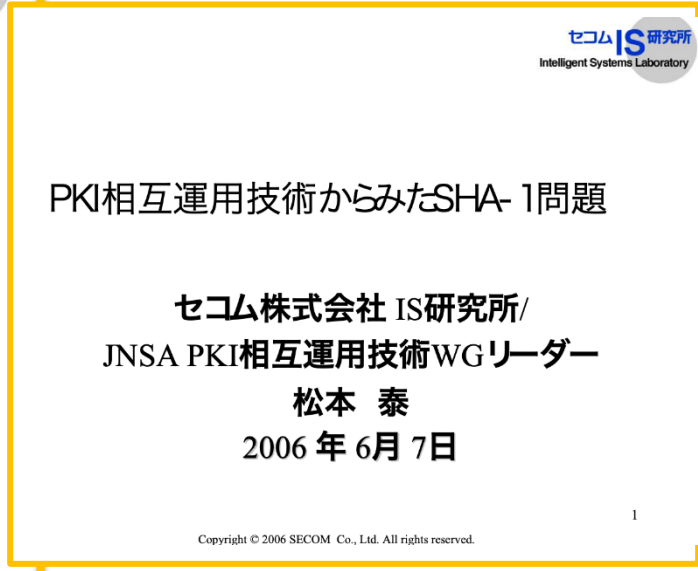
現実の世界

- MSの証明書リストにある107個の自己署名証明書
  - MD5(46個)、MD2(11個)、SHA1(50個)
- 自己署名証明書の有効期間は、10年から20年
- これらは「信頼できる認証局の信頼点」になり得るのか？
  - MD5がダメといいつつMSの「信頼できる認証局の信頼点」を無条件に受け入れてはいないか？。こうしたギャップは埋められるものなのか？

・ どうやって移行（マイグレーション）するのか??誰が全体を取りまとめるか??

- 政策担当者(電子政府など)、暗号関係者、アプリケーション開発ベンダー、認証局、PKI標準化関係者等。これらの2者以上で会話することは極めて稀（3者は皆無、かつ。会話が成り立たない？）

20



セコム IS研究所 Intelligent Systems Laboratory

PKI相互運用技術からみたSHA-1問題

セコム株式会社 IS研究所/
JNSA PKI相互運用技術WGリーダー
松本　泰
2006 年 6月 7日

1

出典：PKI相互運用技術からみたSHA-1問題　2006年6月
https://www.jnsa.org/seminar/2006/20060607/matsumoto_02.pdf

現実の世界？　（2006年当時の状況）

現実の問題　SSL証明書とMD5

セコムIS研究所 Intelligent Systems Laboratory

某サイト

- NI*C
  - https://www2.bits.go.jp/opinion.html
  - SSL証明書　　md5withRSA
  - 自己署名証明書　　md2withRSA

・政府機関の情報セキュリティ対策のための統一基準（2005年項目限定版）

・http://www.bits.go.jp/active/general/pdf/2siryou04-3d.pdf

・(e) 情報システムセキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、アルゴリズムを選択するに当たっては、必要とされる安全性及び信頼性について検討を行い、電子政府推奨暗号リストに記載されたアルゴリズムが選択可能であれば、これを選択すること。ただし、新規（更新を含む。）に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、電子政府推奨暗号リストの中から選択すること。なお、複数のアルゴリズムを選択可能な構造となっている場合には、少なくとも一つを電子政府推奨暗号リストの中から選択すること。

16

電子政府推奨暗号リスト
初版　2003年

↓

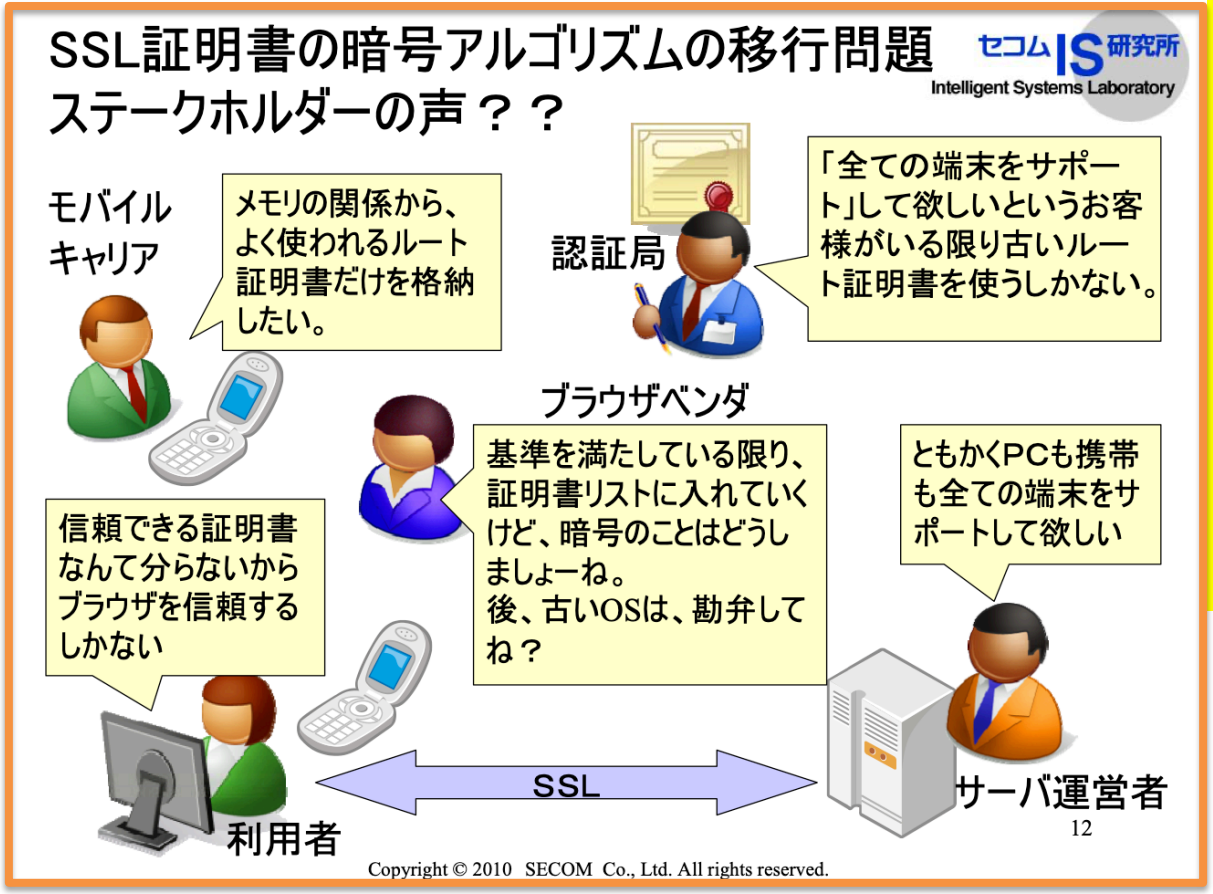
政府機関の情報セキュリティ対策のための統一基準
初版　2005年

↓

政府機関の情報システム
(暗号システムの調達など)

出典：
PKI相互運用技術からみたSHA-1問題　2006年6月
https://www.jnsa.org/seminar/2006/20060607/matsumoto_02.pdf

どうやって移行(マイグレーション)するのか??
誰が全体を取りまとめるか??



レガシーな信頼点（RSA1024）が組み込まれた携帯（ガラケー）をサポートするために、移行は、なかなか進まなかった。

マルチステークホルダー環境の移行は、デットロックとなる可能性が強い。

結局のところ、移行には、何らかの強制力が必要となる。
→ 「2030年問題」も同様

出典：社会基盤としてのPKI / PKIの10年
2010年6月29日
https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf

政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針

2008年4月　（2012年10月に改訂版が発行）

平成 20 年 4 月 22 日
情報セキュリティ政策会議決定

政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針

エ　内閣官房、総務省及び関係府省庁は、新たな暗号アルゴリズムに対応した情報システムの相互運用性の検証を可能とする環境の整備について 2008 年度当初に検討に着手し、2009 年度の構築を目指す。

オ　各府省庁は、上述の検討結果を踏まえ、原則として、2010 年度に新規に構築（更改を含む。以下同じ。）する情報システムから 3(1)の設計要件を組み入れ、2013 年度までに各情報システムを当該要件に適合させるものとする。ただし、2009 年度に構築する情報システムについては、3(1)ウの仕様を適用する。

出典：
政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指
2008年4月
https://www.nisc.go.jp/pdf/policy/general/crypto_pl.pdf

改訂版
2012年10月
https://www.nisc.go.jp/pdf/policy/general/angou_ikoushishin.pdf

- 2008年当時「移行指針」が示されたことは、極めて重要だった。
- 「移行指針」が「2010年暗号移行問題」対応へのトリガーを引いた。
- 実際の移行のスケジュールが明らかになったのは、4年後の2012年の改訂版

H10 次世代暗号アルゴリズムへの移行 ～暗号の2010年問題にどう対応すべきか～

日時

2008年11月27日　09:30～12:30

会場

秋葉原コンベンションホール Room5A

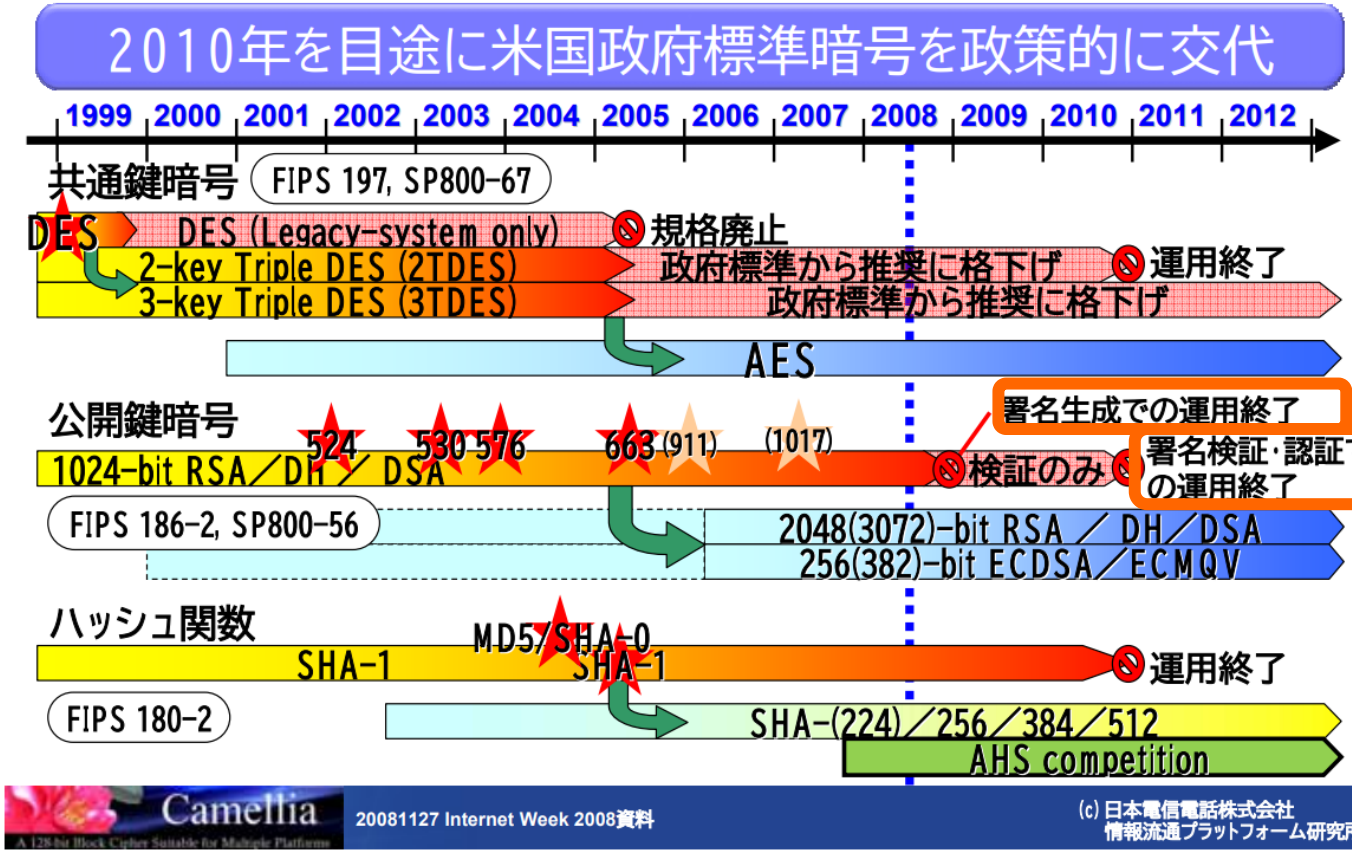
Internet Week 2008
2008.11.25 ▶ 11.28

プログラム紹介ページ

タイトル	講演者	配布資料 (PDF)
2) 暗号アルゴリズムの安全性のお話		
暗号アルゴリズムの安全性のお話	神田 雅透/ＮＴＴ情報流通プラットフォーム研究所	8.52MB
3) 政府機関における安全な暗号利用の促進		
政府機関における安全な暗号利用の促進	繁富 利恵/内閣官房情報セキュリティセンター/産業技術総合研究所情報セキュリティ研究センター	543KB
4) 次世代暗号アルゴリズムへの移行～暗号の2010年問題にどう対応すべきか～		
次世代暗号アルゴリズムへの移行～暗号の2010年問題にどう対応すべきか～	松本 泰/セコム株式会社 IS研究所	1.69MB

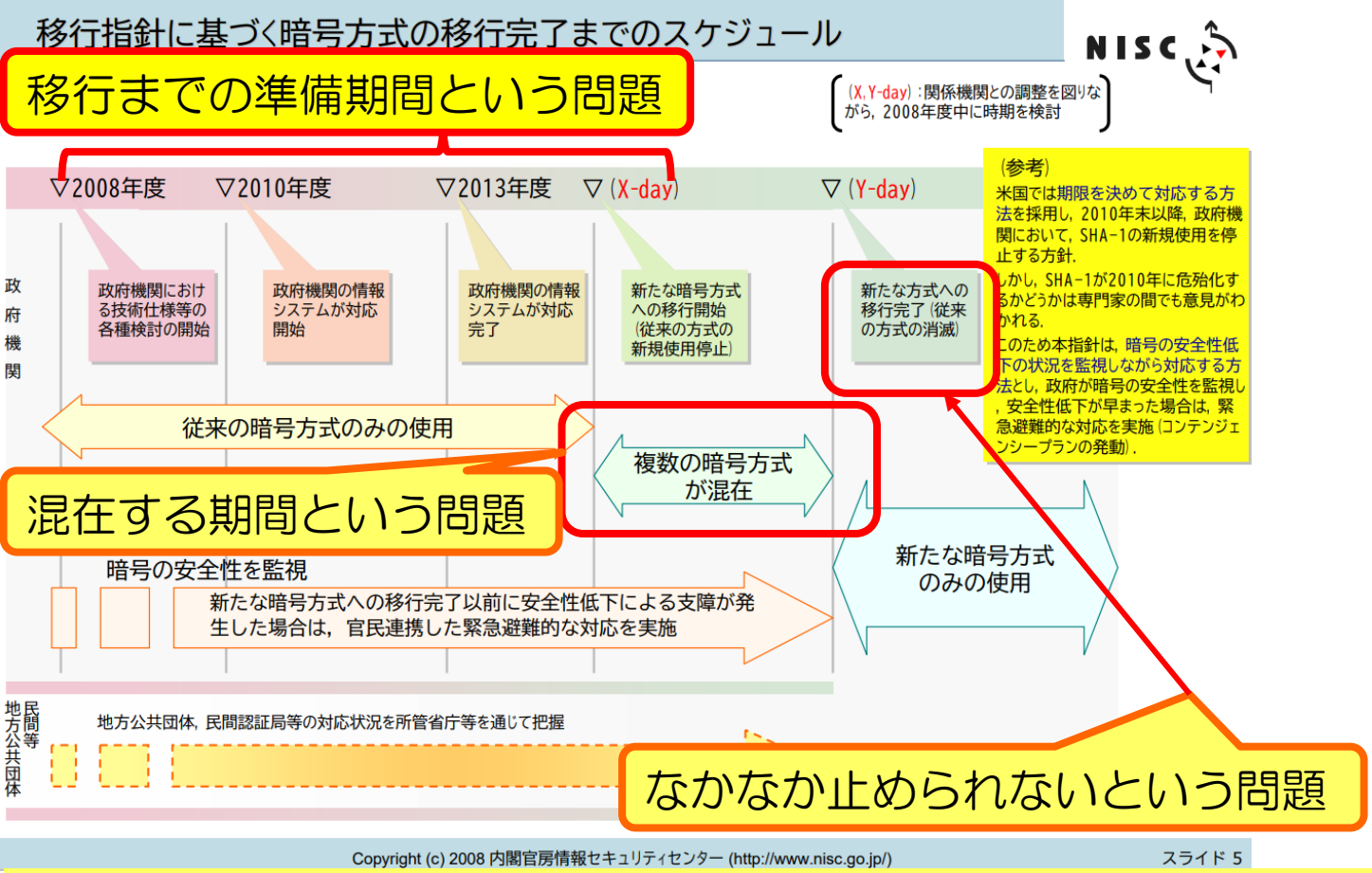
出典: 次世代暗号アルゴリズムへの移行 ～暗号の2010年問題にどう対応すべきか～ 2008年11月
https://www.nic.ad.jp/ja/materials/iw/2008/proceedings/H10/

米国政府の次世代暗号移行政策(’05.8公表)



出典: 次世代暗号アルゴリズムへの移行 ～暗号の2010年問題にどう対応すべきか～ 2008年11月
「暗号アルゴリズムの安全性のお話」
神田 雅透/ＮＴＴ情報流通プラットフォーム研究所
https://www.nic.ad.jp/ja/materials/iw/2008/proceedings/H10/IW2008-H10-01.pdf

2010年問題の2010年（末）は、署名検証の終了のはずだった？？
（Y-day）
署名生成の終了(X-day)は、2008年末



出典：次世代暗号アルゴリズムへの移行 ～暗号の2010年問題にどう対応すべきか～
2008年11月
政府機関における安全な暗号利用の促進
内閣官房情報セキュリティセンター
産業技術総合研究所情報セキュリティ研究センター　繁富 利恵
https://www.nic.ad.jp/ja/materials/iw/2008/proceedings/H10/IW2008-H10-02.pdf

X-day:新たな暗号方式 新たな暗号方式への移行開始 への移行開始（従来の方式の（従来の方式の 新規使用停止）
Y-day:新たな方式への 新たな方式への移行完了（従来 移行完了（従来 の方式の消滅）の方式の消滅

暗号アルゴリズムの移行の議論

セコム IS研究所 Intelligent Systems Laboratory

信頼される安心を、社会へ。 SECOM

出典：
次世代暗号アルゴリズムへの移行 ～暗号の2010年問題にどう対応すべきか～ 2008年11月
松本 泰/セコム株式会社 IS研究所
https://www.nic.ad.jp/ja/materials/iw/2008/proceedings/H10/IW2008-H10-03.pdf

暗号アルゴリズムの歴史

古典暗号 → 現代暗号 → 評価の確立 → 世代交代

IETF, ISO, ITU Etc…

暗号技術を利用した様々な標準化

標準化へのインパクト

電子署名法、Webサーバ証明書の発行、etc….

暗号技術を利用した様々な実装の展開基盤の確立

実装の展開基盤へのインパクト

「半導体」は「産業のコメ」に対して、「暗号技術」は、ありとあらゆるITソリューションに加工され組み込まれる「産業のコムギ」？なので、問題の本質が分かり難い。

暗号は、ITソリューションの「米」じゃなくて「小麦」状態??
ありとあらゆるITソリューションに組み込まれている

公的個人認証サービス（JPKI）における　X-day,Yday

- 2003年　住基カードカード　（RSA1024 with SHA1証明書）発行開始
  - カードの有効期間　10年、（旧）JPKIの証明書の有効期間（3年）
- 2008年　暗号アルゴリズムSHA-1及びRSA1024に係る移行指針　　by NISC
- 2009年　「公的個人認証サービスにおける暗号方式等の移行に関する検討会報告書」の公表
  - 出典：https://www.soumu.go.jp/main_sosiki/kenkyu/kouteki_kojin/index.html
  - 2011年度末を目途に新たな暗号アルゴリズムに対応する住基カードの交付を開始
  - SHA-2及びRSA2048による電子署名についての認証業務を開始する。（2014年度早期まで）
  - →　これらは、実行されず？??（RSA2048withSHA2証明書の発行開始は2016年1月）
- 2013年　マイナンバー法　成立　（2012年　マイナンバー法　廃案）
- 2015年12月末
  - 住基カード発行終了（有効期限は2025/12）。（旧）JPKI証明書発行終了（有効期限は2018/12）
- 2016年1月
  - マイナンバーカード、JPKI（RSA2048対応カード、RSA2048withSHA2証明書）の発行開始
  - マイナンバーカードの発行開始を X-day とした場合、2008年4月の移行指針から約８年弱かかったことになる
- 2018年末
  - （旧）JPKIの証明書の有効期間（3年）　2010年問題のY-day ？？
  - 2018年12月までは、RSA1024の署名生成が行われていた（X-day？）と考えられる。

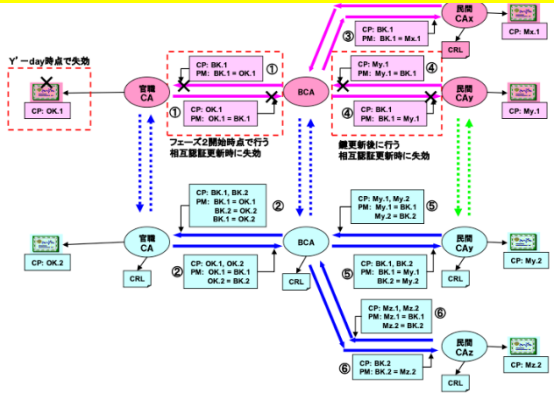
GPKI 政府認証基盤相互運用性仕様書 - GPKI、LGKI、JPKI移行のメカニズム

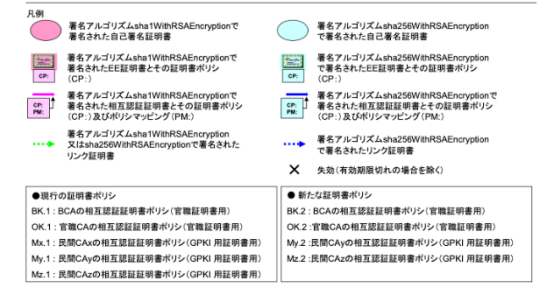
https://www.gpki.go.jp/session/index.html

2.1.2.2. フェーズ2

フェーズ 2 における相互認証証明書の状態は図 2-2のとおりである。

フェーズ2は、２０１０問題の移行期間中





※ 官職 CA と BCA との間の相互認証証明書には、上記の他に利用者証明書の証明書ポリシとポリシマッピングが含まれるが、図では省略している。

図 2-2 フェーズ 2 における相互認証証明書の状態

出典:
政府認証基盤(GPKI) 政府認証基盤相互運用性仕様書 (移行期間編)
https://www.gpki.go.jp/session/CompatibilitySpecifications_phase2.pdf

- 初版は、2001年4月に発行されているが、基本的なアーキテクチャは変更がない。
- 2010年問題の対応を経て現在に至る
  - 暗号技術をベースとした社会基盤となるシステムの寿命は長い
- 基本的にリンク証明書(OldWithNew、NewWithOld）の機能によりGPKI、LGKI、JPKI、商業登記CA、電子署名法の民間CAなど、複数の認証局における新旧暗号アルゴリズムの証明書の混在（および移行）を可能にしている。
  - 「暗号2010年問題」「暗号2030年問題」に対応する移行メカニズムは、2001年の設計当初から備わっている（米国FPKIと同様）
  - しかし、移行には十分な時間を掛ける必要がある。 ->. それぞれのシステム更新、調達などは、非同期に行われる（それぞれのライフサイクルがある）

「2010年暗号移行問題の振り返り」のまとめ

信頼される安心を、社会へ。
SECOM

- 米国政府の当初の2010年の意味
  - X-Dayは、2008年中
  - Y-dayは、2010年末　→ これが、「2010年問題」のはずだった？？
- NISCの移行指針　2008年4月　→ ここで初めて2010年問題対応へのトリガー引かれた
  - X-dayの想定は、　2014年早期
- NISCの移行指針改訂版　2012年10月　移行のスケジュールが具体的に示された
  - X-dayの想定は、　2014年9月下旬以降の早期
  - Y-dayの想定は、　2015 年度まで 、（条件付きで）2019 年度を超えない 範囲
- JPKI証明書における実際の移行
  - X-day　2016年1月　→　移行指針から約8年
  - Y-day　2018年末　→ 2010年（末）問題と言いつつ、2018年（末）
  - 最後の住基カードの有効期限は2025年末　-> 実質的にはマイナンバーカードへ置き換え

2008年の移行指針は、「2010年問題」において非常に重要な役割を果たした。
しかし、この移行指針がトリガーを引いた移行の結末？に関して、関係者間において認識されているとは言えないかもしれない。

欧州における2030年暗号移行問題の対応方針と状況

SOG-ISの暗号評価スキーム・合意された暗号メカニズム

SOG-IS Crypto Working Group

SOG-IS Crypto Evaluation Scheme
Agreed Cryptographic Mechanisms

Document purpose: specify the requirements of the SOG-IS Crypto Evaluation Scheme related to the selection of cryptographic mechanisms. This document is primarily intended for developers and evaluators.

Version 1.3
February 2023

- 欧州のSOG-IS(Senior Officials Group – Information Systems Security) のSOG-IS協定に基づく文書
- アルゴリズムと鍵長などと、その利用期限が明記
  - CRYPTREC 「暗号強度要件(アルゴリズム及び鍵長選択)に 関する設定基準（2022年3月」とも近い文書
- 2016年５月　Ver1.0 発行（最新版は 2023年1月 Ver.1.3）
  - この文書の関連性を維持するために、最先端の進歩を考慮して2年ごとに改訂
- アウトプット先（この文書を参照している）
  - CC（コモンクライテリア）暗号技術利用製品の認証
  - 欧州のeIDAS規則に準拠したETSIのトラストサービス関連の標準文書

出典： SOGIS　Crypto WG – supporting documents
https://www.sogis.eu/uk/supporting_doc_en.html

SOG-ISの暗号評価スキーム・合意された暗号メカニズム

- 二つの種類の「合意された暗号メカニズム」
  - （この文書発行時点で）推奨されるメカニズム　「2030年問題対応」
    - オフライン攻撃に対して少なくとも 125 ビットのセキュリティを提供する必要
      - → RSA2048などは、既に「推奨」ではない！（2016年 V1.0発行時点で）
  - （大規模に展開されている）レガシーメカニズム　「2030年問題非対応」
    - レガシーメカニズムは（期限まで）許容されるがセキュリティマージンが低い
      - → 日本国内は、ほぼ、この大規模に展開されているレガシーメカニズムの状況
- ２年毎に更新　->　レガシーメカニズムの記述が変更
  - 2016(Ver1.0)
    - レガシーメカニズムのデフォルトの受け入れ期限は、2020年(12月31日)
  - 2018(ver1.1)
    - レガシーメカニズムのデフォルトの受け入れ期限は、2022年(12月31日)
  - 2020(ver.1.2)　および　2023(Ver1.3)
    - 「レガシー暗号メカニズム」の記述・定義が変更。暗号アルゴリズム毎の期限
    - RSA2048のレガシーメカニズムは、2025年に合意が取り下げられる

出典： SOGIS　Crypto WG - supporting documents　https://www.sogis.eu/uk/supporting_doc_en.html

耐量子計算機暗号の対応・移行に関する記述

- 2016年版（Ver.1.0）
  - 量子計算機は暗号技術にとって直ちに脅威となるものではないが、将来的にはこのような事態が起こるかもしれない。現在の文書では、合意された量子耐性メカニズムは提供されていない。数年以内に量子耐性メカニズムの標準化が行われる可能性があるため、そのようなメカニズムは将来のバージョンで導入されるかもしれない。
- 2018年版（Ver.1.1）　　2016年版と同様
- 2020年版（Ver.1.2）
  - 先端の暗号メカニズムの安全性を脅かすほど大規模な量子計算機はまだ開発されていないが、非常に活発な取り組みであり、今後数十年のうちに実現されるかもしれないと期待する専門家もいる。本文書では、合意された非対称量子耐性メカニズムを提供しない。そのようなメカニズムについては、現在進行中の安全性評価プロセスを経て、将来のバージョンで導入される予定である。
  - While no quantum computers large enough to threaten the security of state-of-the-art cryptographic mechanisms has been developed yet, it is a very active endeavour, and some experts expect it may be achieved in the coming decades. This current document does not provide agreed asymmetric quantum resistant mechanisms. Such mechanisms will be introduced in future versions, following the ongoing process of assessing the security of such mechanisms.
- 2023年年版（Ver.1.3）　　2020年版（Ver.1.2）と同様

出典：https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf

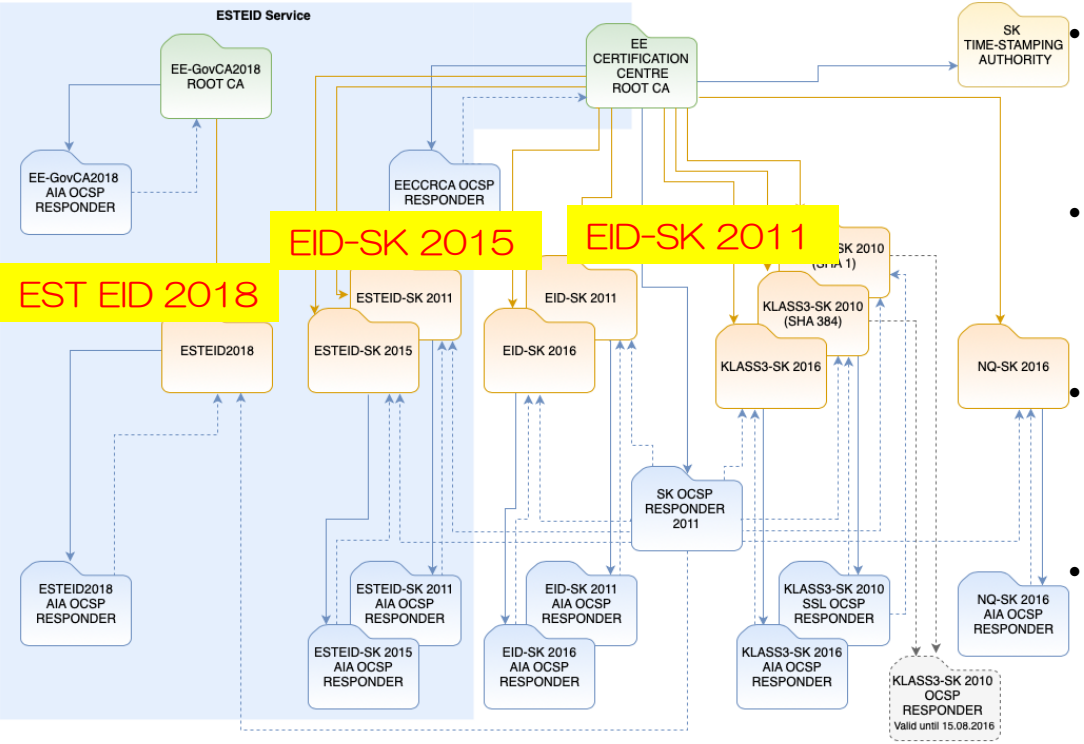
ETSI TS 119 312
Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

出典：
https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.02_60/ts_119312v010402p.pdf

- 欧州のeIDAS規則に準拠したETSIのトラストサービス関連の標準化文書のひとつ　→　　推奨というよりは強制力が働く。
- 暗号メカニズムは、SOG-IS の文書 （２年毎に更新）を参照
  - ETSI TS 119 312 も合わせてに２年毎に更新
- Cryptographic Suites
  - 署名アルゴリズム＋ハッシュ＋パディングの組み合わせのセット
- トラストサービスの標準化、相互運用性確保の観点が目的
  - 相互運用性確保、移行のコスト、実装・展開の容易さ観点からは、Cryptographic Suitesを選定（限定）
  - →　検証環境のコストにも、非常に大きな影響を与える
- 2014年（ETSI TS 119 312 V1.1.1 (2014-11) ）において120bitセキュリティへの移行を促している
  - 2014年時点で、2020年を超える証明書（有効期間が６年以上の証明書）は、RSA 3072bit などを推奨

Cryptographic Suites標準化の意義　→　日本において欠ける標準化という観点の重要性
欧州においては、こうした標準文書に従って、多くの「ビルディングブロック」「オープンソース」が開発され、さまざまな基盤で共通に利用されている。結果、移行も容易になる。

エストニアのeIDの認証局（CA証明書）とeIDの事例
-> 欧州のeIDAS規則のQTSP(クオリファイド・トラストサービスプロバイダー)



出典：
https://www.skidsolutions.eu/en/repository/

- エストニアのeIDは、
  - 2002年発行開始(RSA1024 SHA-1)
  - カード有効期間5年
  - 証明書有効期間5年
- EID-SK 2011　発行開始　2011年
  - EUのトラストリストでは既に無効
  - CA証明書　RSA2048 SHA-1
  - EE証明書　RSA2048 SHA-1
- EID-SK 2015　発行開始　2015年
  - EUのトラストリストにおいて有効
  - CA証明書　RSA4096 SHA-384
  - EE証明書　RSA2048他？？？
- EST EID 2018　発行開始　2018年
  - EUのトラストリストにおいて有効
  - CA証明書　ECDSA SHA-512
  - EE証明書　ECDSA SHA-512

- エストニアのeIDは、既に「2030年問題」をクリア
- SOG-IS、ETSI(eIDAS)など方針に沿った移行に見受けられる

まとめと

-- 2030年問題？とCRYPTRECの果たすべき役割 --

2030年問題？とCRYPTRECの果たすべき役割

- 2003年に公開された「CRYPTREC電子政府推奨暗号リスト」 および、CRYPTRECの活動は、今日のデジタル社会において、非常に大きな役割を果たし貢献したことは間違いない。
- しかし、現在の枠組み（推奨暗号リスト、統一基準ほか）は、2010年問題の対応が長引いたことからも、不足していたと考えられる。→ しかし総括されておらず、この認識に欠ける。
- また、暗号技術が社会基盤としてさらに浸透している中での 2030年問題の対応は、困難なものになることが推測される。
- 2023年7月時点においてETSI TS 119 312 にみられるような相互運用性確保と移行を考慮した「 2030年問題に対応した暗号スイート（Cryptographic Suites）」 が示されていないとこは、今後のデジタル社会の基盤構築に対して大きな障害になる可能性がある（と思う）。
  - サイバー空間とフィジカル空間を高度な融合が目指されているSociety5.0において、暗号技術を使用したシステムは、高度な融合、様々な連携が望まれる。ここでは、検証環境の整備などが重要で、これには、暗号スイートの標準化が欠かせない。
- 「CRYPTREC電子政府推奨暗号リスト」の公開から約20年、今後のCRYPTRECの果たすべき役割も含め、こうした暗号移行問題（耐量子計算機暗号への移行も含めて）への対応の枠組みなどが（欧州の事例なども参考に）検討されるべきではないか。

参考スライド

日本銀行金融研究所ディスカッション・ペーパー
SSL証明書における暗号アルゴリズム移行の現状と今後の対応　　松本　泰、宇根　正志　　2010年4月
https://www.imes.boj.or.jp/research/abstracts/japanese/10-J-11.html

- インターネット上で重要な情報をやり取りする際には、アクセス先のサーバーが正当なサーバーであることを確認する必要がある。仮にサーバーの確認が困難な場合、偽のサイトに誤ってパスワード等の重要な情報を入力してしまうおそれがある。インターネット・バンキング等では、こうした問題への対策として、SSL（Secure Socket Layer）と呼ばれる暗号通信プロトコルによってサーバー認証を行うケースが多い。
- こうしたなか、近年、SSLで利用されている暗号アルゴリズムの安全性低下が顕著になってきている。特に、サーバー認証等に用いられる「SSL証明書」や「ルート証明書」と呼ばれるデータを、より安全性の高い暗号アルゴリズムを利用したものに更新する必要がある。しかしながら、金融機関のサーバーの設定が適切に更新されたとしても、末端の利用者のPCや携帯電話等の設定が更新されなければサーバー認証が実行困難となり、偽サイトにおける情報漏洩等のリスクが残存してしまう。このような状況を回避するためには、サーバー運営者である金融機関をはじめ、末端の利用者、ブラウザー・ベンダー、認証局ベンダー等の関係者が歩調を合わせて対応を検討することが必要である。
- 本稿では、SSL証明書等における暗号アルゴリズムの安全性低下とその移行問題について説明するとともに、SSL証明書やルート証明書の更新を進めていくうえで今後どのような取組みが必要かを検討する。

SSL 証明書の事例に見る暗号アルゴリズムの移行問題 2011年

——収束しない 2010 年問題——

島岡　政基[†a)]　　松本　泰[†]

暗号技術を利用した情報通信技術が基盤化するほどに，この暗号アルゴリズムの移行は困難なものになる

Issues on Transition of Cryptographic Algorithm Learned from a Case Study of SSL Certificates

Masaki SHIMAOKA[†a)] and Yasushi MATSUMOTO[†]

あらまし　社会基盤化しつつある現代の情報通信は，暗号技術なくしては成り立たない．しかし，この暗号技術が情報通信に広く取り込まれたのは，それほど古い話ではなく，今後解決すべき課題も数多く残されている．その課題の一つに暗号アルゴリズムの移行問題がある．情報通信に広く取り込まれた暗号技術であるが，ここで利用されている暗号アルゴリズムは，徐々に脆弱化していき，世代交代が必要になっている．情報通信技術や情報通信基盤は，こうした暗号アルゴリズムの世代交代に伴う移行に対応できる必要がある．しかし暗号技術を利用した情報通信技術が基盤化するほどに，この暗号アルゴリズムの移行は困難なものになると予想される．本論文では，既に広く利用されている SSL 及び SSL 証明書の事例を示すことにより移行問題の複雑さと重要さを説明するとともに，今後の取り組むべき課題について考察を行う．

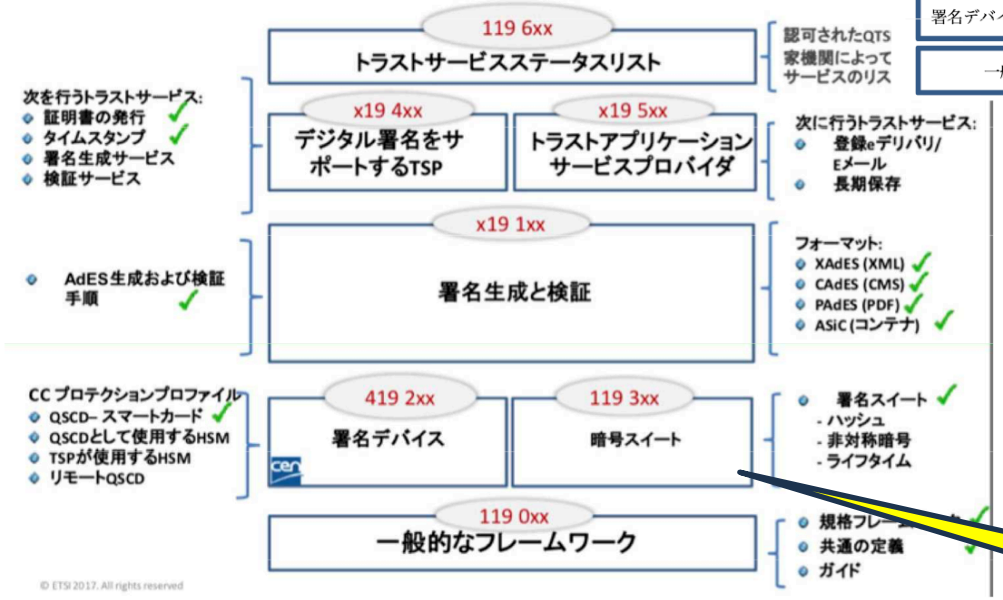
キーワード　暗号アルゴリズム，暗号移行可能性，ルート証明書，SSL 証明書，認証局

出典：
https://search.ieice.org/bin/pdf_link.php?category=B&lang=J&year=2011&fname=j94-b_1_1&abst=

ETSI TS 119 312 Cryptographic Suitesの位置付け

ETSIとCENが開発した「欧州標準」 EN

- 非常によく体系化され整備されている
- 法的な要求との整合が、よく考慮されている（法的相互運用性）
- 詳細な技術仕様からテストまでが仕様化されている（相互運用性の確保と実装可能、利用される標準）



出典：https://itc.jipdec.or.jp/common/images/kouensiryou_4.pdf

ETSI TS 119 312

EUの技術標準
-- デジタル単一市場戦略の中核となるトラスト –
松本 泰 セコム(株)IS研究所
2019年 2月 7日
https://itresearchart.biz/19ws207/docs/s03.pdf

ETSI TS 119 312 Cryptographic Suitesの記述

信頼される安心を、社会へ。
SECOM

ETSI TS 102 176-1 V2.1.1 (2011-07)

Table 7: Recommended parameters for RSA and rsagen1 for a resistance during X years

Parameter	1 year	3 years	6 years	10 years (speculative)
MinModLen	1 536	2 048	2 048	?
ErrProb	2^{-80}	2^{-100}	2^{-100}	2^{-100}
SeedEntropy/EntropyBits	80	100	100	?

出典： https://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.01.01_60/ts_10217601v020101p.pdf

ETSI TS 119 312 V1.1.1 (2014-11)

Table 7: Recommended parameters for RSA and rsagen1 for a resistance during X years

Parameter	1 year	3 years	6 years	10 years (speculative)
MinModLen	1 536	2 048	3 072	4 096
ErrProb	2^{-80}	2^{-100}	2^{-100}	2^{-120}
SeedEntropy/EntropyBits	80	100	100	?

出典： https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf

2014年から認証局のCA証明書の移行が始まった

ETSI TS 119 312 V1.2.1 (2017-05)

Table 6: Recommended parameters for RSA for a resistance during X years

Parameter	1 year	3 years	6 years
Key size ($\log_2(n)$)	≥ 1 900	≥ 1 900	≥ 3 000

出典： https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.02.01_60/ts_119312v010201p.pdf

RSAに関しては、ETSI TS 119 312 V1.4.2 (2022-02)の記述も同様

最新版　ETSI TS 119 312 V1.4.2 (2022-02)

https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.02_60/ts_119312v010402p.pdf

Cryptographic Suitesの記述

Table 4: List of signature suites

Entry name of the signature suite	Entry name for the hash function	Entry name for the signature algorithm	SOGIS-recommended/ legacy ([14], p. 28)
sha224-with-rsa	SHA-224	RSA-PKCSv1_5	L
sha256-with-rsa	SHA-256	RSA-PKCSv1_5	L
sha384-with-rsa	SHA-384	RSA-PKCSv1_5	L
sha512-with-rsa	SHA-512	RSA-PKCSv1_5	L
rsa-pss with mgf1SHA-256Identifier	SHA-256	RSA-PSS	R
rsa-pss with mgf1SHA-384Identifier	SHA-384	RSA-PSS	R
rsa-pss with mgf1SHA-512Identifier	SHA-512	RSA-PSS	R
rsa-pss with mgf1SHA3-Identifier	SHA3-256, SHA3-384 or SHA3-512	RSA-PSS	R
sha224-with-ecdsa	SHA-224	EC-DSA	L
sha2-with-ecdsa	SHA-256, SHA-384 or SHA-512	EC-DSA	R
sha2-with-ecsdsa	SHA-256, SHA-384 or SHA-512	EC-SDSA-opt	R
sha3-with-ecdsa	SHA3-256, SHA3-384 or SHA3-512	EC-DSA	R
sha3-with-ecsdsa	SHA3-256, SHA3-384 or SHA3-512	EC-SDSA-opt	R

L　レガシー
R　推奨

最新版　ETSI TS 119 312 V1.4.2 (2022-02)

https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.02_60/ts_119312v010402p.pdf

Cryptographic Suitesの記述

Table 9: Recommended signature suites for algorithm resistance during X years (was table 12 in version 1.1.1)

Entry name of the signature suite	1 year	3 years	6 years
sha256-with-rsa	≥ 1 900	≥ 1 900	not recommended
sha384-with-rsa	≥ 1 900	≥ 1 900	not recommended
sha512-with-rsa	≥ 1 900	≥ 1 900	not recommended
rsa-pss with mgf1SHA-256Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-384Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-512Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA3-Identifier	≥ 1 900	≥ 1 900	≥ 3 000
sha256-with-dsa	2 048	2 048	3 072
sha512-with-dsa	2 048	2 048	3 072
sha224-with-ecdsa	legacy		not recommended
sha2-with-ecdsa	recommended		
sha2-with-ecsdsa	recommended		
sha3-with-ecdsa	recommended		
sha3-with-ecsdsa	recommended		

Table 10: Recommended signature suites for a resistance up to year X

Entry name of the signature suite	2023	2024	2025	after 2025
sha256-with-rsa	≥ 1 900	≥ 1 900	≥ 1 900	≥ 3 000
sha384-with-rsa	≥ 1 900	≥ 1 900	≥ 1 900	≥ 3 000
sha512-with-rsa	≥ 1 900	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-256Identifier	≥ 1 900	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-384Identifier	≥ 1 900	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-512Identifier	≥ 1 900	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA3-Identifier	≥ 1 900	≥ 1 900	≥ 1 900	≥ 3 000
sha256-with-dsa	2 048	2 048	2 048	3 072
sha512-with-dsa	2 048	2 048	2 048	3 072
sha224-with-ecdsa	legacy		not recommended	
sha2-with-ecdsa	recommended			
sha2-with-ecsdsa	recommended			
sha3-with-ecdsa	recommended			
sha3-with-ecsdsa	recommended			

Table 8: Recommended parameters for EC-DSA and EC-SDSA-opt for a resistance during X years

Parameter	1 year	3 years	6 years
pLen = qLen	256, 384 or 512	256, 384 or 512	256, 384 or 512