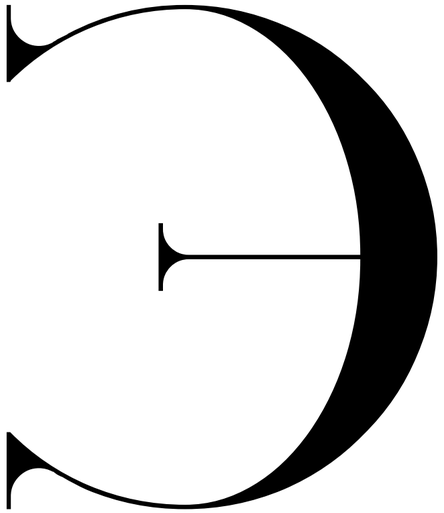

ЭКВИВАЛЕНТНЫЙ

уровень надежности электронной подписи при трансграничном взаимном признании

UNCITRAL

MODEL LAW ON ELECTRONIC SIGNATURES

ТИПОВОЙ ЗАКОН ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

Статья 12. Признание иностранных сертификатов и электронных подписей

1. При определении того, обладает ли — или в какой мере обладает — сертификат или электронная подпись юридической силой, не учитываются:
a) место выдачи сертификата или создания или использования электронной подписи; или
b) местонахождение коммерческого предприятия эмитента или подписавшего.

2. Сертификат, выданный за пределами [принимающего государства], обладает такой же юридической силой в [принимающем государстве], как и сертификат, выданный в [принимающем государстве], **если он обеспечивает по существу ЭКВИВАЛЕНТНЫЙ УРОВЕНЬ НАДЕЖНОСТИ**

3. Электронная подпись, созданная или используемая за пределами [принимающего государства], обладает такой же юридической силой в [принимающем государстве], как и электронная подпись, созданная или используемая в [принимающем государстве], **если она обеспечивает по существу ЭКВИВАЛЕНТНЫЙ УРОВЕНЬ НАДЕЖНОСТИ**

4. При определении того, обеспечивает ли сертификат или электронная подпись по существу эквивалентный уровень надежности для целей пункта2 или 3, следует учитывать **признанные международные стандарты** и любые другие соответствующие факторы.

5. В тех случаях, когда, независимо от положений пунктов 2, 3 и 4, стороны договариваются между собой об использовании определенных видов электронных подписей или сертификатов, такая договоренность признается достаточной для цели трансграничного признания, за исключением случаев, когда такая договоренность не будет действительной или не будет иметь силы согласно применимому праву.

Статья 6. Соблюдение требования в отношении наличия подписи

3.ЭЛЕКТРОННАЯ ПОДПИСЬ СЧИТАЕТСЯ **НАДЕЖНОЙ** ..., ЕСЛИ:

a) данные для создания электронной подписи в том контексте, в котором они используются, связаны с подписавшим и ни с каким другим лицом;

b) данные для создания электронной подписи в момент подписания находились под контролем подписавшего и никакого другого лица;

c) любое изменение, внесенное в электронную подпись после момента подписания, поддается обнаружению; и

d) в тех случаях, когда одна из целей юридического требования в отношении наличия подписи заключается в гарантировании целостности информации, к которой она относится, любое изменение, внесенное в эту информацию после момента подписания, поддается обнаружению.

Статья 10. Надежность

...ПРИ ОПРЕДЕЛЕНИИ ТОГО, ЯВЛЯЮТСЯ ЛИ – ИЛИ В КАКОЙ МЕРЕ ЯВЛЯЮТСЯ – ЛЮБЫЕ СИСТЕМЫ, ПРОЦЕДУРЫ И ЛЮДСКИЕ РЕСУРСЫ, ИСПОЛЬЗУЕМЫЕ ПОСТАВЩИКОМ СЕРТИФИКАЦИОННЫХ УСЛУГ, **НАДЕЖНЫМИ**, МОГУТ УЧИТЫВАТЬСЯ СЛЕДУЮЩИЕ ФАКТОРЫ:

a) финансовые и людские ресурсы, в том числе наличие активов;

b) качество систем аппаратного и программного обеспечения;

c) процедуры для обработки сертификатов и заявок на сертификаты и хранения записей;

d) наличие информации для подписавших, идентифицированных в сертификатах, и для потенциальных полагающихся сторон;

e) регулярность и объем аудита, проводимого независимым органом;

f) наличие заявления, сделанного государством, аккредитующим органом или поставщиком сертификационных услуг в отношении соблюдения или наличия вышеуказанного; или

g) любые другие соответствующие факторы.

Статья 12. Соблюдение требования в отношении наличия подписи

"ПО СУЩЕСТВУ ЭКВИВАЛЕНТНЫЙ УРОВЕНЬ НАДЕЖНОСТИ"

...в пункте 2 устанавливается пороговый уровень технического соответствия иностранных сертификатов, основанный на сопоставлении степени их надежности в сравнении с требованиями в отношении надежности, установленными принимающим государством согласно Типовому закону

...требование эквивалентности, как оно используется в пункте2, не означает, что уровень надежности иностранного сертификата должен быть абсолютно идентичным уровню надежности внутреннего сертификата

...при применении понятия эквивалентности ... следует учитывать, что эквивалентность должна устанавливаться между функционально сопоставимыми сертификатами.

факторы, которые следует учитывать при оценке эквивалентности иностранных сертификатов и подписей по существу уже перечислены в статьях 6, 9 и 10. Кроме того, в пункте 4 учитываются последствия того факта, что оценка эквивалентности иностранных сертификатов несколько отличается от оценки надежности поставщика сертификационных услуг согласно статьям 9 и 10.

понятие "признанный международный стандарт" следует толковать широко – как охватывающее международные технические и коммерческие стандарты, а также стандарты и нормы, принятые правительственными или межправительственными органами и "добровольные стандарты"

Method	Date	Symmetric	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
[1] Lenstra / Verheul	2022	87	1995 1568	154	1995	164	174
[2] Lenstra Updated	2022	83	1446 1660	166	1446	166	166
[3] ECRYPT	2018 - 2028	128	3072	256	3072	256	256
[4] NIST	2019 - 2030	112	2048	224	2048	224	224
[5] ANSSI	2021 - 2030	128	2048	200	2048	256	256
[6] NSA	-	256	3072	-	-	384	384
[7] RFC3766	-	-	-	-	-	-	-
[8] BSI	2020 - 2022	128	2000	250	2000	250	256

All key sizes are provided in bits. These are the minimal sizes for security.

Author: Damien Giry
Approved by Prof. Jean-Jacques Quisquater
Contact: keylength@bluekrypt.com

I would like to thank Prof. Arjen K. Lenstra for his kind authorization and comments.
Surveys of laws and regulations on cryptology: Crypto Law Survey / Digital Signature Law Survey.

Bibliography

[1] Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal Of Cryptology, vol. 14, p. 255-293, 2001.
[2] Key Lengths, Arjen K. Lenstra, The Handbook of Information Security, 06/2004.
[3] Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018.
[4] Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5, NIST, 05/2020.
[5] Mécanismes cryptographiques - Règles et recommandations, Rev. 2.03, ANSSI , 02/2014.
[6] Commercial National Security Algorithm, National Security Agency (NSA), 01/2016.
[7] Determining Strengths for Public Keys Used for Exchanging Symmetric Keys, RFC 3766, H. Orman and P. Hoffman, 04/2004.
[8] Cryptographic Mechanisms: Recommendations and Key Lengths, TR-02102-1 v2020-01, BSI, 03/2020.

сертификата, и результаты проверки действительности сертификата;

1.3. установление доверия к сертификату, изданному поставщиком услуг иностранного государства, осуществляется республиканским унитарным предприятием «Национальный центр электронных услуг» (далее – предприятие) и включает в себя оценку:

порядка выработки, хранения, резервного копирования, восстановления, депонирования, использования личного ключа электронной цифровой подписи;

порядка регистрации конечных пользователей, издания сертификатов и списков отозванных сертификатов, отзыва, приостановления, возобновления действия сертификатов, предоставления информации о статусе сертификатов;

наличия инфраструктуры, необходимой для оказания услуг по управлению сертификатами;

используемых средств электронной цифровой подписи, криптографических алгоритмов и механизмов, протоколов информационного взаимодействия, форматов обмена данными;

управления операционной деятельностью, системным доступом, внедрением и обслуживанием безопасных доверенных информационных систем, восстановлением при сбоях и обеспечением непрерывности деятельности, безопасностью персонала, физической защитой и защитой от воздействий окружающей среды, защитой информации с учетом актуальных угроз безопасности информации и действий нарушителя в соответствии с законодательством иностранного государства;

порядка и условий прекращения деятельности поставщика услуг иностранного государства.

По результатам оценки предприятием с поставщиком услуг иностранного государства