Лекция 4. Криптографические примитивы: ЭЦП

Косолапов Ю.В.

ЮФУ

24 сентября 2020 г.

Содержание

Виды подписи

Виды электронной подписи [1]

[1] Федеральный закон от 06.04.11 № 63-ФЗ «Об электронной подписи»

Виды подписи

Виды электронной подписи [1]

- **Простая подпись** – подтверждает подписание электронного документа определенным лицом, однако не гарантирует неизменность файла после подписания (пароли, одноразовые пароли в SMS).

[1] Федеральный закон от 06.04.11 № 63-ФЗ «Об электронной подписи»

Виды подписи

Виды электронной подписи [1]

- **Простая подпись** – подтверждает подписание электронного документа определенным лицом, однако не гарантирует неизменность файла после подписания (пароли, одноразовые пароли в SMS).
- **Неквалифицированная электронная подпись** позволяет определить автора документа и проверить, были ли внесены в файл какие-либо изменения после его отправки. Подписанный с ее помощью документ заменяет бумажный документ только в случаях, оговоренных законом, или по согласию сторон (используются криптографические алгоритмы).

[1] Федеральный закон от 06.04.11 № 63-ФЗ «Об электронной подписи»

Виды подписи

Виды электронной подписи [1]

- **Простая подпись** – подтверждает подписание электронного документа определенным лицом, однако не гарантирует неизменность файла после подписания (пароли, одноразовые пароли в SMS).
- **Неквалифицированная электронная подпись** позволяет определить автора документа и проверить, были ли внесены в файл какие-либо изменения после его отправки. Подписанный с ее помощью документ заменяет бумажный документ только в случаях, оговоренных законом, или по согласию сторон (используются криптографические алгоритмы).
- **Квалифицированная электронная подпись** (КЭП) позволяет определить автора документа и проверить, были ли внесены в файл какие-либо изменения после его отправки. Документ, подписанный с помощью сертификата КЭП, приравнивается к документу, который собственноручно подписан физическим лицом или уполномоченным представителем юридического лица.

[1] Федеральный закон от 06.04.11 № 63-ФЗ «Об электронной подписи»

Виды подписи

Виды электронной подписи [1]

- **Простая подпись** – подтверждает подписание электронного документа определенным лицом, однако не гарантирует неизменность файла после подписания (пароли, одноразовые пароли в SMS).
- **Неквалифицированная электронная подпись** позволяет определить автора документа и проверить, были ли внесены в файл какие-либо изменения после его отправки. Подписанный с ее помощью документ заменяет бумажный документ только в случаях, оговоренных законом, или по согласию сторон (используются криптографические алгоритмы).
- **Квалифицированная электронная подпись** (КЭП) позволяет определить автора документа и проверить, были ли внесены в файл какие-либо изменения после его отправки. Документ, подписанный с помощью сертификата КЭП, приравнивается к документу, который собственноручно подписан физическим лицом или уполномоченным представителем юридического лица.
  - Есть удостоверяющий центр (УЦ), который обязательно подтверждает квалифицированную подпись.

[1] Федеральный закон от 06.04.11 № 63-ФЗ «Об электронной подписи»

Виды подписи

Виды электронной подписи [1]

- **Простая подпись** – подтверждает подписание электронного документа определенным лицом, однако не гарантирует неизменность файла после подписания (пароли, одноразовые пароли в SMS).
- **Неквалифицированная электронная подпись** позволяет определить автора документа и проверить, были ли внесены в файл какие-либо изменения после его отправки. Подписанный с ее помощью документ заменяет бумажный документ только в случаях, оговоренных законом, или по согласию сторон (используются криптографические алгоритмы).
- **Квалифицированная электронная подпись** (КЭП) позволяет определить автора документа и проверить, были ли внесены в файл какие-либо изменения после его отправки. Документ, подписанный с помощью сертификата КЭП, приравнивается к документу, который собственноручно подписан физическим лицом или уполномоченным представителем юридического лица.
  - Есть удостоверяющий центр (УЦ), который обязательно подтверждает квалифицированную подпись.
- Под ЭЦП мы будем понимать НЭП и КЭП.

[1] Федеральный закон от 06.04.11 № 63-ФЗ «Об электронной подписи»

ЭЦП на основе симметричных шифров и хэш-функций

Условия:

ЭЦП на основе симметричных шифров и хэш-функций

Условия:

1. участник A намерен передать участнику B сообщение $\mathbf{m} \in \{0,1\}^*$ (оно может быть несекретным), при этом B хочет убедиться, что полученное сообщение создал именно A и оно не было изменено;

ЭЦП на основе симметричных шифров и хэш-функций

Условия:

1. участник A намерен передать участнику B сообщение $\mathbf{m} \in \{0,1\}^*$ (оно может быть несекретным), при этом B хочет убедиться, что полученное сообщение создал именно A и оно не было изменено;
2. оригинальное сообщение отправителя и подпись обозначим $(\mathbf{m}, \mathbf{s})$, а принятые получателем сообщение и подпись — $(\mathbf{m}', \mathbf{s}')$;

ЭЦП на основе симметричных шифров и хэш-функций

Условия:

1. участник A намерен передать участнику B сообщение $\mathbf{m} \in \{0,1\}^*$ (оно может быть несекретным), при этом B хочет убедиться, что полученное сообщение создал именно A и оно не было изменено;
2. оригинальное сообщение отправителя и подпись обозначим $(\mathbf{m}, \mathbf{s})$, а принятые получателем сообщение и подпись — $(\mathbf{m}', \mathbf{s}')$;
3. участники A и B должны обладать общим секретным ключом $\mathbf{k} \in \{0,1\}^m$, $m \geqslant 128$.

На основе криптографической хэш-функции $h : \{0,1\}^* \to \{0,1\}^n$, $n \geqslant 128$:

ЭЦП на основе симметричных шифров и хэш-функций

Условия:

1. участник A намерен передать участнику B сообщение $\mathbf{m} \in \{0,1\}^*$ (оно может быть несекретным), при этом B хочет убедиться, что полученное сообщение создал именно A и оно не было изменено;
2. оригинальное сообщение отправителя и подпись обозначим $(\mathbf{m}, \mathbf{s})$, а принятые получателем сообщение и подпись — $(\mathbf{m}', \mathbf{s}')$;
3. участники A и B должны обладать общим секретным ключом $\mathbf{k} \in \{0,1\}^m$, $m \geqslant 128$.

На основе криптографической хэш-функции $h : \{0,1\}^* \to \{0,1\}^n$, $n \geqslant 128$:

- Плохой способ:

$$A \to B : \mathbf{m}, h(\mathbf{m}) = \mathbf{s}$$

$$B : h(\mathbf{m}') \stackrel{?}{=} \mathbf{s}'$$

ЭЦП на основе симметричных шифров и хэш-функций

Условия:

1. участник A намерен передать участнику B сообщение $\mathbf{m} \in \{0,1\}^*$ (оно может быть несекретным), при этом B хочет убедиться, что полученное сообщение создал именно A и оно не было изменено;
2. оригинальное сообщение отправителя и подпись обозначим $(\mathbf{m}, \mathbf{s})$, а принятые получателем сообщение и подпись — $(\mathbf{m}', \mathbf{s}')$;
3. участники A и B должны обладать общим секретным ключом $\mathbf{k} \in \{0,1\}^m$, $m \geqslant 128$.

На основе криптографической хэш-функции $h : \{0,1\}^* \to \{0,1\}^n$, $n \geqslant 128$:

- Плохой способ:

$$A \to B : \mathbf{m}, h(\mathbf{m}) = \mathbf{s}$$

$$B : h(\mathbf{m}') \stackrel{?}{=} \mathbf{s}'$$

- Хороший способ:

$$A \to B : \mathbf{m}, h(\mathbf{m} \parallel \mathbf{k}) = \mathbf{s}$$

$$B : h(\mathbf{m}' \parallel \mathbf{k}) \stackrel{?}{=} \mathbf{s}'$$

ЭЦП на основе симметричных шифров и хэш-функций

На основе блочного шифра с алгоритмами шифрования/расшифрования $\mathbf{E}, \mathbf{D} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$:

ЭЦП на основе симметричных шифров и хэш-функций

На основе блочного шифра с алгоритмами шифрования/расшифрования $\mathbf{E}, \mathbf{D} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$:

- Плохой способ:

$$
\begin{aligned}
A \to B :& E_{\mathbf{k}}(\mathbf{m} \parallel h(\mathbf{m})) = \mathbf{s}(\text{сообщение содержится в подписи}) \\
B :& D_{\mathbf{k}}(\mathbf{s}') = (\mathbf{m}', h') \\
B :& h(\mathbf{m}') \stackrel{?}{=} h'
\end{aligned}
$$

ЭЦП на основе симметричных шифров и хэш-функций

На основе блочного шифра с алгоритмами шифрования/расшифрования $\mathbf{E}, \mathbf{D} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$:

- Плохой способ:

$$\begin{aligned} A \to B :& E_{\mathbf{k}}(\mathbf{m} \parallel h(\mathbf{m})) = \mathbf{s} (\text{сообщение содержится в подписи}) \\ B :& D_{\mathbf{k}}(\mathbf{s}') = (\mathbf{m}', h') \\ B :& h(\mathbf{m}') \stackrel{?}{=} h' \end{aligned}$$

Подвержен *truncation*-атаке со стороны противника M:

$$\begin{aligned} M \to A(*) :& \mathbf{m}_2 = \mathbf{m} \parallel h(\mathbf{m}) \parallel \mathbf{m}_1 \\ A \to M(**) :& E_{\mathbf{k}}(\mathbf{m}_2) = E_{\mathbf{k}}(\mathbf{m} \parallel h(\mathbf{m}) \parallel \mathbf{m}_1 \parallel h(\mathbf{m}_2)) = \mathbf{s} \\ M :& \mathbf{s} = \mathbf{s}_1 \parallel \mathbf{s}_2, \mathbf{s}_1 = E_{\mathbf{k}}(\mathbf{m} \parallel h(\mathbf{m})) \\ M \to B(***) :& \mathbf{s}_1 \\ B :& D_{\mathbf{k}}(\mathbf{s}_1) = (\mathbf{m}, h = h(\mathbf{m})) \\ B :& (h(\mathbf{m}) \stackrel{?}{=} h) = True. \end{aligned}$$

ЭЦП на основе симметричных шифров и хэш-функций

На основе блочного шифра с алгоритмами шифрования/расшифрования $\mathbf{E}, \mathbf{D} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$:

ЭЦП на основе симметричных шифров и хэш-функций

На основе блочного шифра с алгоритмами шифрования/расшифрования $\mathbf{E}, \mathbf{D} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$:

- Хороший способ:

$$
\begin{aligned}
A \to B &: \mathbf{m}, E_{\mathbf{k}}(h(\mathbf{m})) = \mathbf{s} \\
B &: D_{\mathbf{k}}(\mathbf{s}') = h' \\
B &: h(\mathbf{m}') \stackrel{?}{=} h'
\end{aligned}
$$

ЭЦП на основе симметричных шифров и хэш-функций

На основе блочного шифра с алгоритмами шифрования/расшифрования $\mathbf{E}, \mathbf{D} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$:

- Хороший способ:

$$\begin{aligned} A \to B &: \mathbf{m}, E_{\mathbf{k}}(h(\mathbf{m})) = \mathbf{s} \\ B &: D_{\mathbf{k}}(\mathbf{s}') = h' \\ B &: h(\mathbf{m}') \stackrel{?}{=} h' \end{aligned}$$

Замечание 1

Подпись на основе симметричных шифров и хэш-функций используется, как правило, только в кругу участников взаимодействия, **доверяющих друг другу**. Почему?

ЭЦП на основе симметричных шифров и хэш-функций

На основе блочного шифра с алгоритмами шифрования/расшифрования $\mathbf{E}, \mathbf{D} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$:

- Хороший способ:

$$\begin{aligned} A \to B &: \mathbf{m}, E_{\mathbf{k}}(h(\mathbf{m})) = \mathbf{s} \\ B &: D_{\mathbf{k}}(\mathbf{s}') = h' \\ B &: h(\mathbf{m}') \stackrel{?}{=} h' \end{aligned}$$

Замечание 1

Подпись на основе симметричных шифров и хэш-функций используется, как правило, только в кругу участников взаимодействия, **доверяющих друг другу**. Почему?

Замечание 2

Такая подпись обычно называется **имитовставкой** (в российских стандартах) или MAC (message authentication code) — код аутентификации сообщения.

Общие идеи

Пусть имеется асимметричный шифр, $\mathbf{k}_p$ – публичный (открытый) ключ, $\mathbf{k}_s$ – секретный (закрытый) ключ.

Общие идеи

Пусть имеется асимметричный шифр, $\mathbf{k}_p$ – публичный (открытый) ключ, $\mathbf{k}_s$ – секретный (закрытый) ключ.

Идея 1

Так как секретный ключ $\mathbf{k}_s$ известен только тому участнику, который генерировал пару $(\mathbf{k}_s, \mathbf{k}_p)$, то с помощью этого ключа можно попытаться как-то генерировать подпись для документа.

Сложность нахождения $\mathbf{k}_s \sim$ Сложность подделки подписи.

Общие идеи

Пусть имеется асимметричный шифр, $\mathbf{k}_p$ – публичный (открытый) ключ, $\mathbf{k}_s$ – секретный (закрытый) ключ.

Идея 1

Так как секретный ключ $\mathbf{k}_s$ известен только тому участнику, который генерировал пару $(\mathbf{k}_s, \mathbf{k}_p)$, то с помощью этого ключа можно попытаться как-то генерировать подпись для документа.

Сложность нахождения $\mathbf{k}_s \sim$ Сложность подделки подписи.

Идея 2

Так как публичный ключ $\mathbf{k}_p$ известен ВСЕМ, то с помощью этого ключа можно попытаться как-то проверять корректность подписи.

Проверка прошла успешно с помощью $\mathbf{k}_p \sim$ Документ не был изменен.

ЭЦП на основе RSA

Шифр RSA:

- Публичный ключ: $\mathbf{k}_p = (e, n)$
- Секретный ключ: $\mathbf{k}_s = (d)$
- Шифрование: $\mathbf{m}^e \mathrm{mod} n = \mathbf{C}$
- Расшифрование: $\mathbf{c}^d \mathrm{mod} n = \mathbf{m}$

ЭЦП на основе RSA

Шифр RSA:

- Публичный ключ: $\mathbf{k}_p = (e, n)$
- Секретный ключ: $\mathbf{k}_s = (d)$
- Шифрование: $\mathbf{m}^e \mathrm{mod} n = \mathbf{C}$
- Расшифрование: $\mathbf{c}^d \mathrm{mod} n = \mathbf{m}$

Наблюдение:

ЭЦП на основе RSA

Шифр RSA:

- Публичный ключ: $\mathbf{k}_p = (e, n)$
- Секретный ключ: $\mathbf{k}_s = (d)$
- Шифрование: $\mathbf{m}^e \mathrm{mod} n = \mathbf{C}$
- Расшифрование: $\mathbf{c}^d \mathrm{mod} n = \mathbf{m}$

Наблюдение:

- Так как шифрование и расшифрование выполняется одинаково (только числа разные), то можно зашифровать секретным, а расшифровать открытым!

ЭЦП на основе RSA

Шифр RSA:

- Публичный ключ: $\mathbf{k}_p = (e, n)$
- Секретный ключ: $\mathbf{k}_s = (d)$
- Шифрование: $\mathbf{m}^e \mathrm{mod} n = \mathbf{C}$
- Расшифрование: $\mathbf{c}^d \mathrm{mod} n = \mathbf{m}$

Наблюдение:

- Так как шифрование и расшифрование выполняется одинаково (только числа разные), то можно зашифровать секретным, а расшифровать открытым!
- Только зашифровывать сможет только владелец секретного ключа, а расшифровывать смогут все!

ЭЦП на основе RSA

Шифр RSA:

- Публичный ключ: $\mathbf{k}_p = (e, n)$
- Секретный ключ: $\mathbf{k}_s = (d)$
- Шифрование: $\mathbf{m}^e \mathrm{mod} n = \mathbf{C}$
- Расшифрование: $\mathbf{c}^d \mathrm{mod} n = \mathbf{m}$

Наблюдение:

- Так как шифрование и расшифрование выполняется одинаково (только числа разные), то можно зашифровать секретным, а расшифровать открытым!
- Только зашифровывать сможет только владелец секретного ключа, а расшифровывать смогут все!
- Для защиты конфиденциальности это не подойдет, а для подписи – самое то!

ЭЦП на основе RSA

Владелец секретного ключа: A (то есть пару $(\mathbf{k}_s, \mathbf{k}_p)$ генерировал A)

ЭЦП на основе RSA

Владелец секретного ключа: A (то есть пару $(\mathbf{k}_s, \mathbf{k}_p)$ генерировал A)

- Избыточный вариант:

$$A \to B : \mathbf{m}(\in \mathbb{Z}_n), \mathbf{s} = \mathbf{m}^d \bmod n$$

$$B : (\mathbf{s}')^e \bmod n \stackrel{?}{=} \mathbf{m}'$$

ЭЦП на основе RSA

Владелец секретного ключа: A (то есть пару $(\mathbf{k}_s, \mathbf{k}_p)$ генерировал A)

- Избыточный вариант:

$$A \to B : \mathbf{m}(\in \mathbb{Z}_n), \mathbf{s} = \mathbf{m}^d \bmod n$$

$$B : (\mathbf{s}')^e \bmod n \stackrel{?}{=} \mathbf{m}'$$

- Неизбыточный вариант (на основе криптографической хэш-функции $h : \{0,1\}^* \to \{0,1\}^m$, $m \leqslant |n|_2$):

$$A \to B : \mathbf{m}(\in \{0,1\}^*), \mathbf{s} = (h(\mathbf{m}))^d \bmod n$$

$$B : (\mathbf{s}')^e \bmod n \stackrel{?}{=} h(\mathbf{m}')$$

ЭЦП на основе RSA

Проблема

В приведенной схеме проверяющая сторона должна знать публичный ключ отправителя (ключ проверки)!

ЭЦП на основе RSA

Проблема

В приведенной схеме проверяющая сторона должна знать публичный ключ отправителя (ключ проверки)!

Плохое решение (отправка с сообщением ключа проверки):

$$A \to B : \mathbf{m}(\in \{0,1\}^*), \mathbf{s} = (h(\mathbf{m}))^d \bmod n, \mathbf{k}_p = (e, n)$$

$$B : (\mathbf{s}')^e \bmod n \stackrel{?}{=} h(\mathbf{m}')$$

ЭЦП на основе RSA

Проблема

В приведенной схеме проверяющая сторона должна знать публичный ключ отправителя (ключ проверки)!

Плохое решение (отправка с сообщением ключа проверки):

$$A \to B : \mathbf{m}(\in \{0,1\}^*), \mathbf{s} = (h(\mathbf{m}))^d \bmod n, \mathbf{k}_p = (e, n)$$

$$B : (\mathbf{s}')^e \bmod n \stackrel{?}{=} h(\mathbf{m}')$$

$$M \to B : \mathbf{m}(\in \{0,1\}^*), \mathbf{s} = (h(\mathbf{m}))^d \bmod n_M, \mathbf{k}_p = (e_M, n_M)$$

$$B : (\mathbf{s}')^{e_M} \bmod n_M \stackrel{?}{=} h(\mathbf{m}')$$

Сертификат публичного ключа

Сертификат публичного ключа

Определение

Сертификат публичного ключа — это документ, содержащий сведения о владельце публичного ключа, криптографических алгоритмах, в которых используется этот ключ, назначение ключа. Этот документ подписан (содержит цифровую подпись) удостоверяющего центра (центра доверия).

Сертификат публичного ключа

Определение

Сертификат публичного ключа — это документ, содержащий сведения о владельце публичного ключа, криптографических алгоритмах, в которых используется этот ключ, назначение ключа. Этот документ подписан (содержит цифровую подпись) удостоверяющего центра (центра доверия).

Назначение удостоверяющего центра

Обратившись в УЦ, можно запросить сертификат любого пользователя и проверить корректность подписи на документе, полученном от этого пользователя.

Сертификат публичного ключа

$$(*)A : (\mathbf{k}_p^A, \mathbf{k}_s^A)$$

$$(*)A \to CA : \mathbf{k}_p^A, D^A = \text{данные владельца}$$

$$(*)CA \to A : \text{Cert}_A = (\mathbf{k}_p^A, D^A, < meta >, \mathbf{s}^{CA,A} = \text{SIGN}_{\mathbf{k}_s^{CA}}(\mathbf{k}_p^A, D^A, < meta >))$$

$$A \to B : \mathbf{m}, \mathbf{s}^{A,B}, \text{Cert}_A$$

$$B : \text{VERIF}_{\mathbf{k}_p^{CA}}(\text{Cert}_A)$$

$$B : \text{VERIF}_{\mathbf{k}_p^A}(\mathbf{m}', \mathbf{s}')$$

Сертификат публичного ключа

$$(*)A : (\mathbf{k}_p^A, \mathbf{k}_s^A)$$

$$(*)A \to CA : \mathbf{k}_p^A, D^A = \text{данные владельца}$$

$$(*)CA \to A : \text{Cert}_A = (\mathbf{k}_p^A, D^A, < meta >, \mathbf{s}^{CA,A} = \text{SIGN}_{\mathbf{k}_s^{CA}}(\mathbf{k}_p^A, D^A, < meta >))$$

$$A \to B : \mathbf{m}, \mathbf{s}^{A,B}, \text{Cert}_A$$

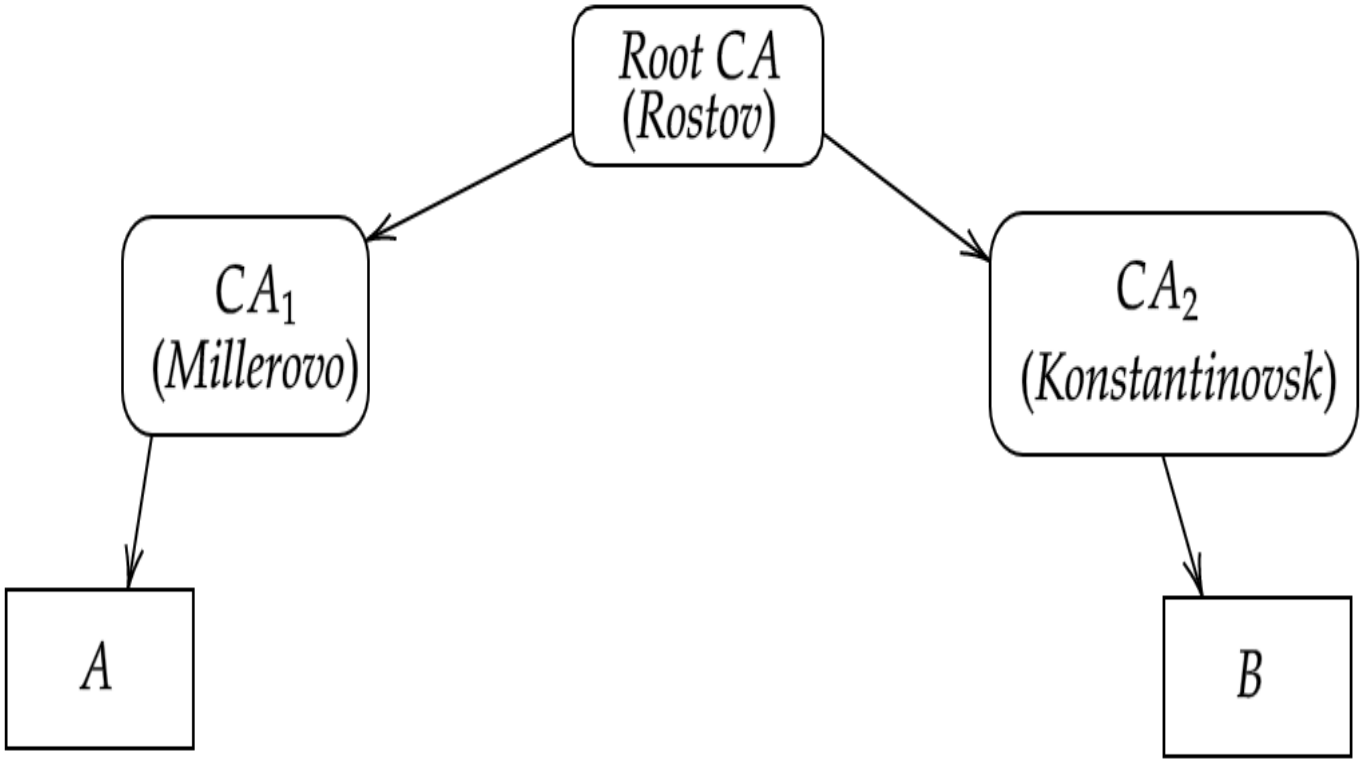
$$B : \text{VERIF}_{\mathbf{k}_p^{CA}}(\text{Cert}_A)$$

$$B : \text{VERIF}_{\mathbf{k}_p^A}(\mathbf{m}', \mathbf{s}')$$

Проблема

В приведенной схеме проверяющая сторона должна знать сертификат удостоверяющего центра!

Пример инфраструктуры открытых ключей



Примеры сертификатов

DEMO

Заключение

Спасибо за внимание!