Стандартная процедура проверки документов:

Стандартная процедура проверки документов:

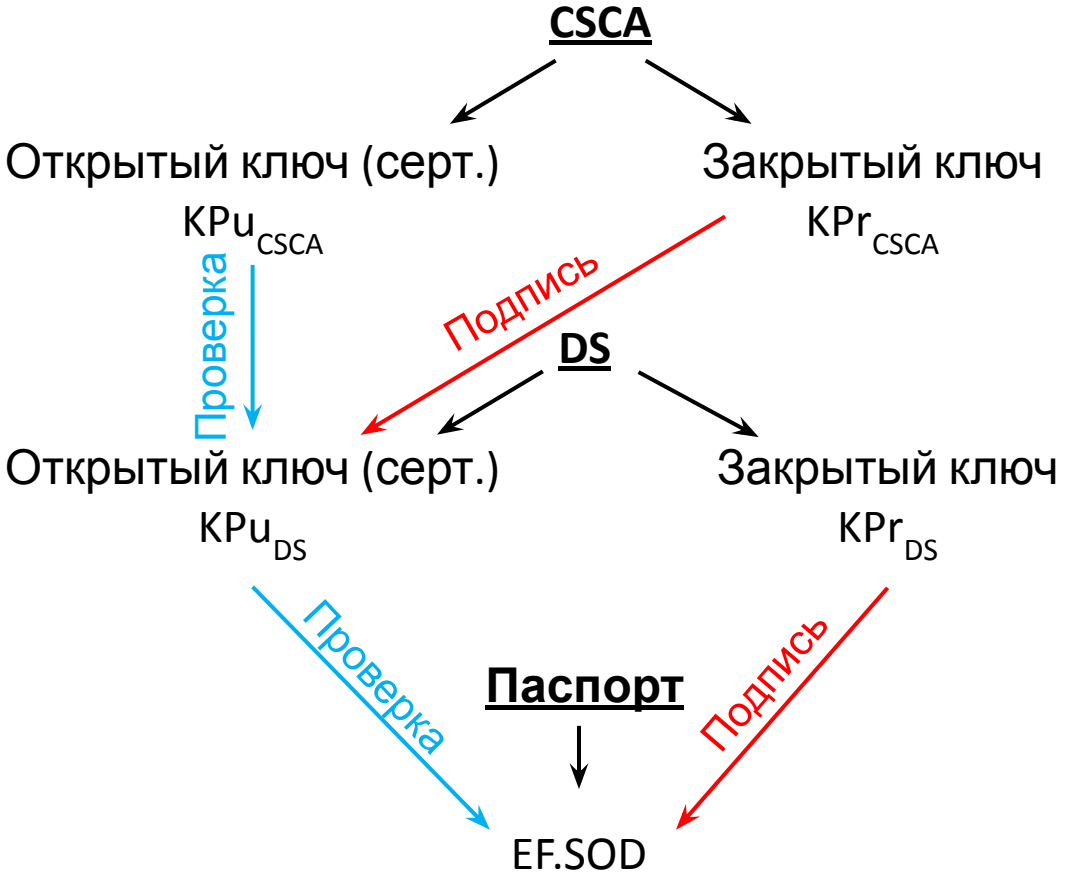
1) BAC (conditional?)
2) PA
3) AA (опционально)
4) Чтение документа

Улучшенная процедура проверки документов:

Стандартная процедура проверки документов:

1) BAC
2) CA
3) PA
4) AA (опционально)
5) TA (conditional?)

Дерево сертификатов PKI - 1



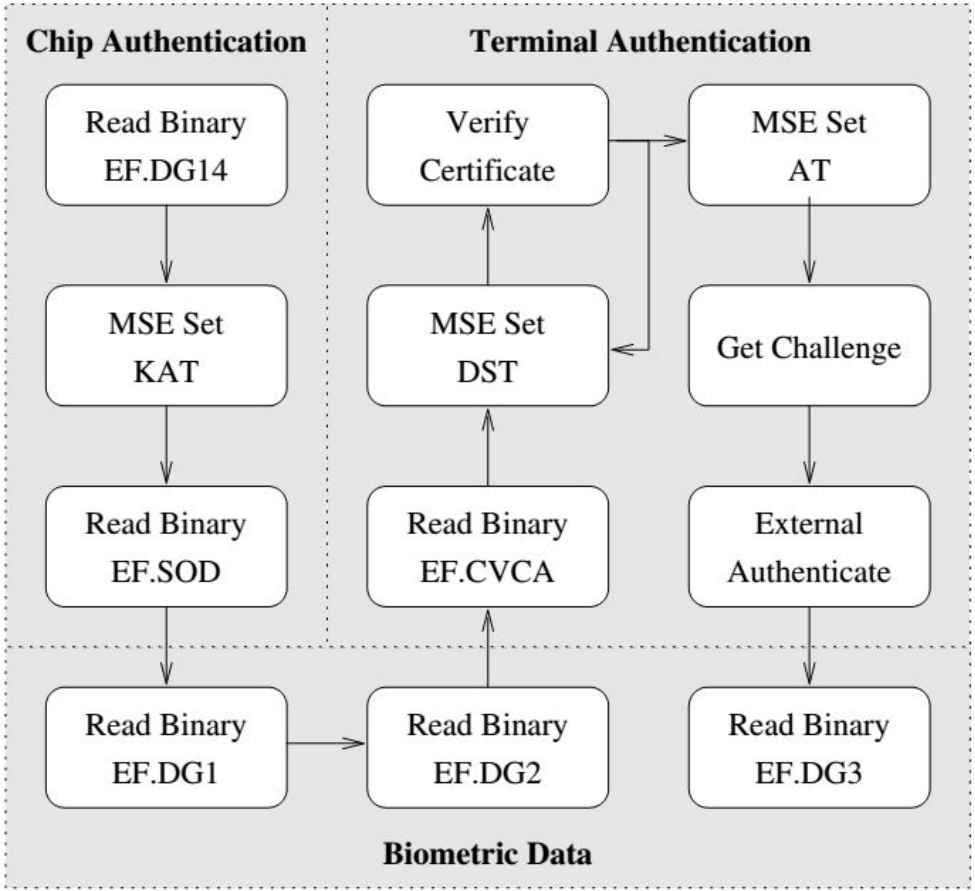


Figure B.1: Command Flow

Аутентификация чипа

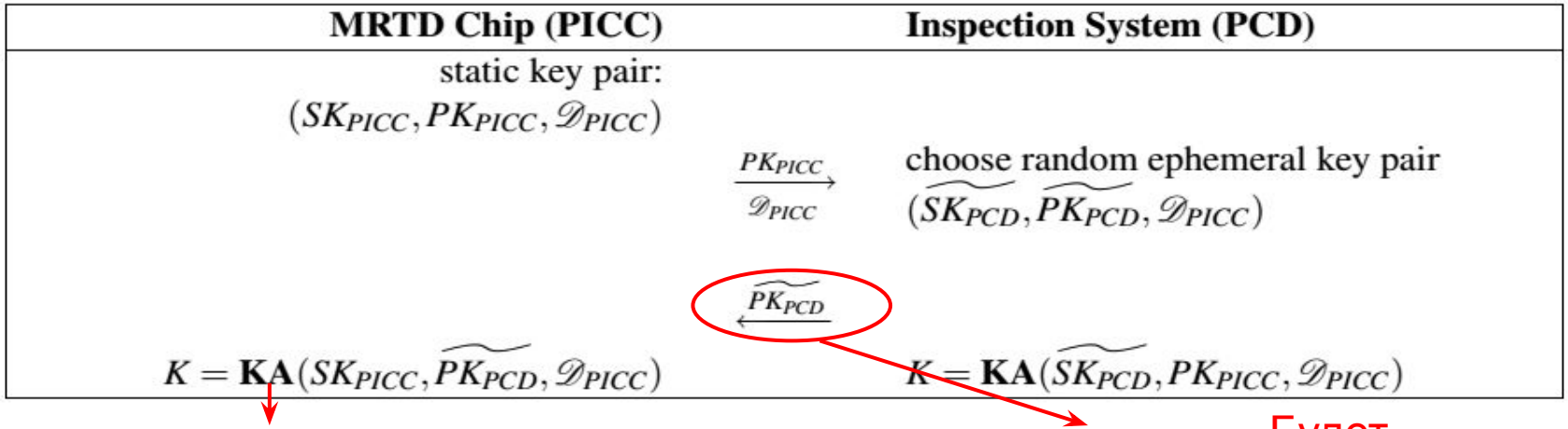


Figure 3.1: Chip Authentication

Алгоритм Диффи-Хеллмана

Будет использоваться при аутентификации терминала

Затем выполняется ПА, позволяющая проверить аутентичность открытого ключа чипа PK_{PICC} (хранится в DG14).

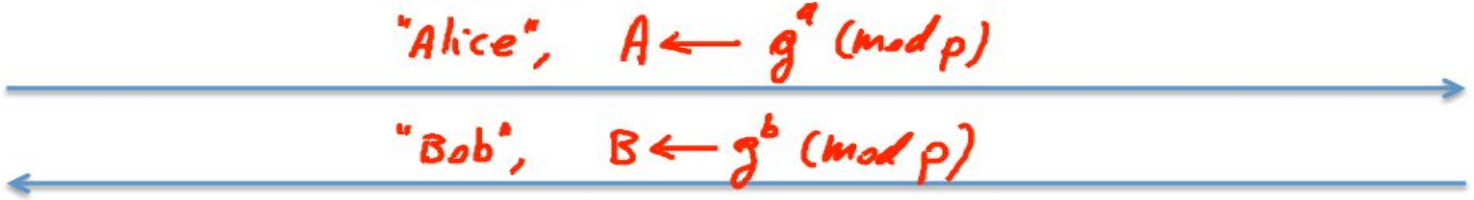
The Diffie-Hellman protocol (informally)

Fix a large prime p (e.g. 600 digits)

Fix an integer g in {1, …, p}

Alice **Bob**

choose random **a** in {1,…,p-1} choose random **b** in {1,…,p-1}



$$B^a \pmod p = (g^b)^a = k_{AB} = g^{ab} \pmod p = (g^a)^b = A^b \pmod p$$

Дерево сертификатов PKI - 2

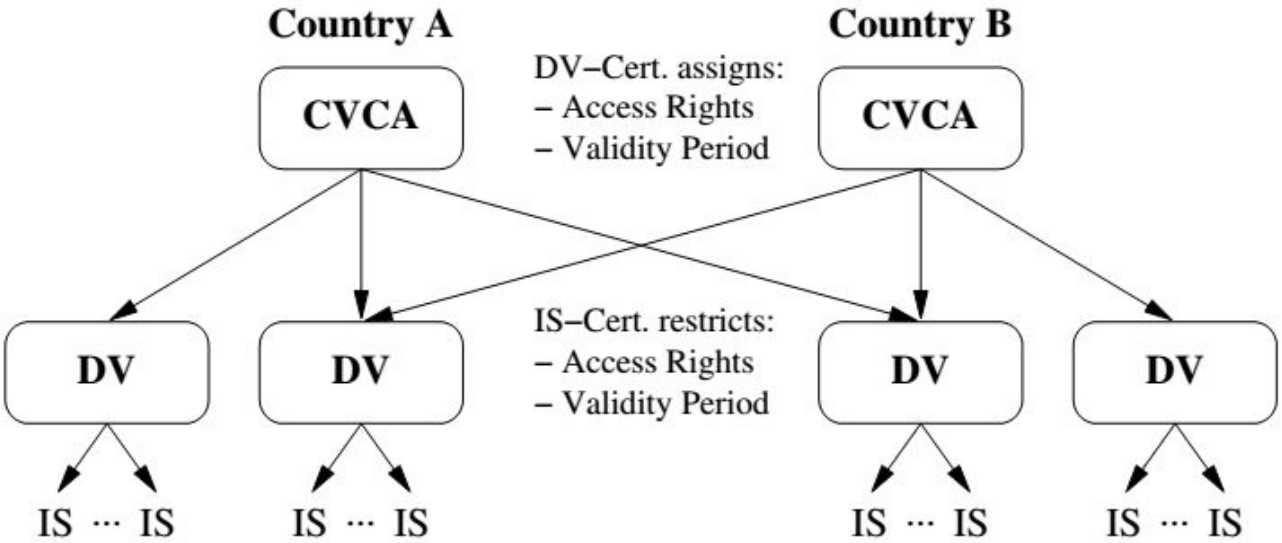


Figure 2.1: Public Key Infrastructure

Аутентификация терминала

Инсп.система (ИС) отправляет чипу последовательность сертификатов, начиная с сертификата, проверяемого открытым ключом CVCA (EF.CVCA), который хранится на чипе, и заканчивая сертификатом ИС.
Чип проверяет сертификаты и извлекает открытый ключ ИС.
Далее выполняются следующие действия:

MRTD Chip (PICC)		Inspection System (PCD)
choose r_{PICC} randomly	$\xrightarrow{r_{PICC}}$	
	$\xleftarrow{s_{PCD}}$	$s_{PCD} = \mathbf{Sign}(SK_{PCD}, ID_{PICC} \| r_{PICC} \| H(\widetilde{PK_{PCD}}))$
$\mathbf{Verify}(PK_{PCD}, s_{PCD}, ID_{PICC} \| r_{PICC} \| H(\widetilde{PK_{PCD}}))$		

Figure 3.2: Terminal Authentication

Стандартная процедура проверки документов:

Стандартная процедура проверки документов:

1) BAC (conditional?)
2) PA
3) AA (опционально)
4) Чтение документа

Улучшенная процедура проверки документов:

Стандартная процедура проверки документов:

1) BAC
2) CA
3) PA
4) AA (опционально)
5) TA (conditional?)

Вопросы:

- CVCA link Certificaters?