Advanced Web Security

Electronic Payments

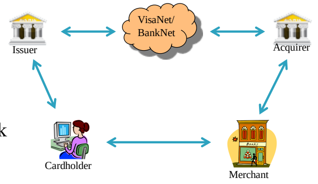
Part 1

Outline

- Card transactions
  - Card-Present
    - Smart Cards
  - Card-Not-Present
    - SET
    - 3D Secure
    - Tokenization
- Untraceable E-Cash
- Micropayments
  - Payword
  - Electronic Lottery Tickets
  - Peppercoin
- Bitcoin/blockchain

Cards

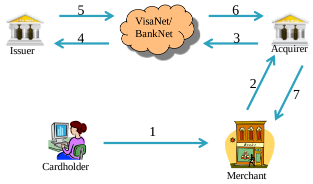
- Credit card or Debit card
- Involved parties
  - Cardholder
  - Merchant
  - Issuer – The Cardholder's Bank
  - Acquirer – The Merchant's Bank
  - The Network
    - VisaNet for Visa
    - BankNet for MasterCard
- For American Express, Discover Card, JCB and Diner's club, the issuer and the acquirer are the same
  - Some have agreements with e.g., MasterCard
  - We do not consider them here



Card Payment Processing

Phase 1, Authorization

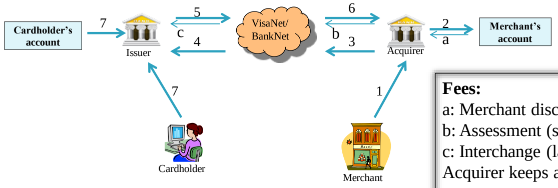
1. Cardholder presents card to Merchant
2. Merchant requests authorization from Acquirer
3. Authorization forwarded to Network
4. Network knows where to find Issuer and asks for authorization
5. Issuer sends authorization response to Network
6. Network forwards it to the Acquirer
7. Acquirer forwards it to the Merchant



Card Payment Processing

Phase 2, Clearing and Settlement

1. Merchant sends approved authorizations to Acquirer (sent in a batch)
2. Acquirer credits Merchant's account and takes a fee
3. Bank sends authorization to the Network
4. Network requests money from the issuer
5. Issuer sends money to Network
6. Network sends money to Bank and takes a fee
7. Cardholder pays invoice or has money directly debited her account with Issuer



Fees:
a: Merchant discount (All)
b: Assessment (small)
c: Interchange (large)
Acquirer keeps a-b-c (small)

Transactions

- Transactions can be one of
  - Card-Present Transaction (CP)
  - Card-Not-Present Transaction (CNP)
- Two important security checks
  - The card must not be a copy of a ”real” card
  - The cardholder must be the true owner

Card-Present Transactions

- Cardholder, Card and Merchant are at the same place when purchase is made
  - Physical stores, Hotels
  - Card reader is typically used, magnetic stripe cards started to appear in the 60's
- Magnetic stripe cards, security features
  - Check that card is valid
    - Physical protection, e.g., hologram
    - Card verification value (CVV1) – code on the magnetic stripe (verified by issuer)
  - Cardholder verification
    - Signature
    - Possible: PIN – stored with issuer, provides two-factor authentication
- Reading the magnetic stripe + knowing PIN is often enough to use card
  - Skimming

1958

Smart Cards

- EMV (Europay, MasterCard, Visa)
- Since Jan 1, 2005 (in Europe): Acquiring bank (Merchants) are responsible for fraud when EMV cards are not used.
  - Before it was the issuer's bank that was liable
  - Reason to change to EMV
  - Liability shift in the U.S.: October 2015
- Important features
  - Difficult to copy
  - Tamper resistant
  - Secure storage
  - Cryptographical computations
  - Based on standards
  - Common Criteria evaluation
  - Still, cheap

Smart Cards (EMV cards)

- Example of card-present transaction
- Quite complex standard

- Three main security features
  - Data authentication – make sure that data on the card is valid
  - Cardholder verification – make sure that cardholder is true owner
  - Transaction authorization – verify that transaction is allowed

EMV: Data authentication

- Card authentication

- Three variants for offline data authentication
  - **Static data authentication (SDA)** – fixed issuer generated signature
  - **Dynamic data authentication (DDA)** – dynamic card generated signature (including nonce from terminal)
  - **Combined DDA/generate application cryptogram (CDA)** – DDA but also signing the cryptogram used to authorize the transaction

EMV: Cardholder Verification

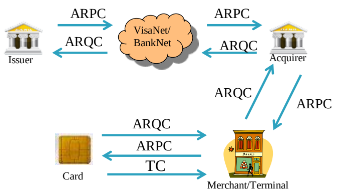
- Cardholder can be verified in several ways
- Examples
  - Online PIN – PIN is sent encrypted to issuer
  - Offline PIN – Card verifies that PIN is ok
  - Signature – Cardholder provides normal signature
  - No CVM required – Can be used for low value transaction

CVM List	
Online PIN	if terminal supports
Signature	attended cash
No CVM required	below $5

Take highest applicable in list

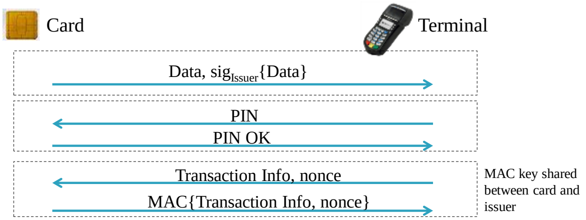
EMV: Transaction authorization

- Terminal requests a cryptogram
- Offline: Card authorizes transaction
  - Generates a transaction certificate (TC)
- Online: Issuer authorizes transaction
  - Generate an *authorization request cryptogram* (ARQC) which terminal sends to issuer
  - Issuer responds with *authorization response cryptogram* (ARPC)
  - Card generates TC which is sent to issuer and saved by merchant
  - Message encrypted with key shared by issuer and card



Attacking EMV

- SDA cards



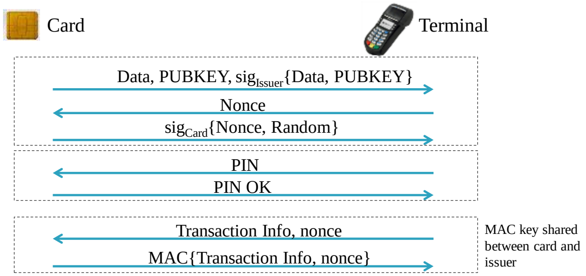
Card
Terminal
Data, sig$_{Issuer}${Data}
PIN
PIN OK
Transaction Info, nonce
MAC{Transaction Info, nonce}
MAC key shared between card and issuer

- Consider all stages offline
- Possible attack?
- Record static authentication data, always answer PIN OK
  - Make your own card, no secrets needed
  - Will not work for online authorization

Called ”Yes card”

Attacking EMV

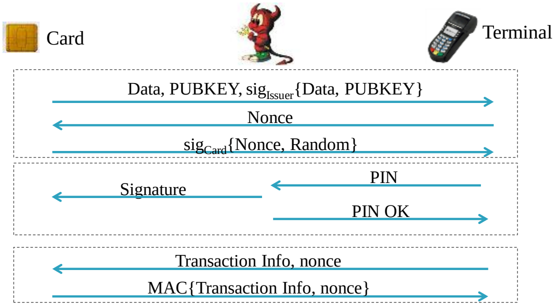
- We make a better card: Use DDA and Online authorization



Card
Terminal
Data, PUBKEY, sig$_{Issuer}${Data, PUBKEY}
Nonce
sig$_{Card}${Nonce, Random}
PIN
PIN OK
Transaction Info, nonce
MAC{Transaction Info, nonce}
MAC key shared between card and issuer

- Possible attack now?

Man-In-The-Middle Attack



Card
Terminal
Data, PUBKEY, sig$_{Issuer}${Data, PUBKEY}
Nonce
sig$_{Card}${Nonce, Random}
Signature
PIN
PIN OK
Transaction Info, nonce
MAC{Transaction Info, nonce}

- ”PIN OK” is not authenticated in the protocol
- Attack will not work for online PIN verification, but successful in e.g., U.K.
- For details, see Murdoch et. al. – Chip and PIN is broken

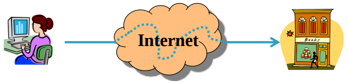
Card-Not-Present Transaction

- Mail/Telephone/Fax/Internet
- Important to verify that Alice is in possession of card and that she is the owner of the card
- Typically two ways
  - Verify billing address – Alice must present the billing address of the card
    - Address Verification System (AVS)
  - Provide information on card
    - Expiry date
    - CVV2/CVC2/CID – this also checks that card is valid
- Verification code is not technically needed but typically gives Merchant less problem in case of chargebacks
  - Merchants are typically liable for CNP transactions

CVV2

Internet transactions

- Often, e-commerce is defined as purchasing over Internet
- Card-not-present transaction over Internet
- SSL/TLS makes a very good starting point.
  - High security
  - Free to use
  - Built into web browsers
- However, Merchant will have access to card information
  - PAN: Personal Account Number
  - CVV2
  - Dates
- Secure Electronic Transaction (SET) was first published in 1997
  - This technology separates internet payments from MOTO

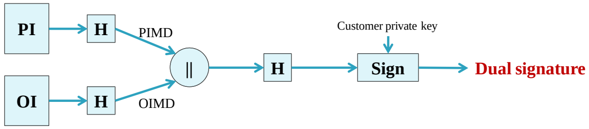


SET

- Initiated by Visa and MasterCard with several large companies involved
  - Protocol is now dead, but it provides several important lessons
- Aims to separate payment information and order information
  - Card number not given to Merchant
- PI = Payment information – Only given to Issuer
- OI = Order information – Only given to Merchant
- Three parties involved
  - Cardholder
  - Merchant
  - Payment gateway

Dual signature

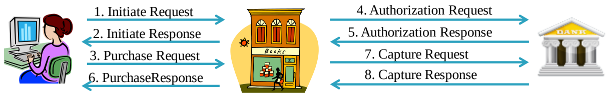
- Concept introduced in SET



- Let Merchant see OI and PIMD
  - PI and OI linked together, but Merchant cannot see PI

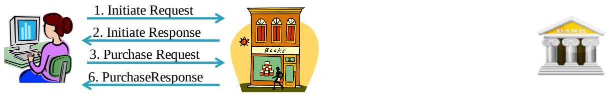
SET Purchase

- Divided into
  - purchase request
  - payment authorization
  - payment capture (just finishing the actual payment, we skip this part)
- All parties have public/private key pair and a corresponding certificate



Purchase Request

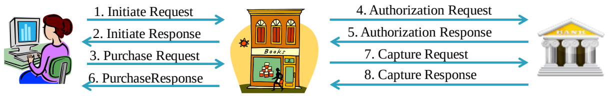
- **Initiate Request** – Cardholder requests Merchant and Payment Gateway’s certificates
- **Initiate Response** – Merchant returns certificates and a signed Transaction ID
- Cardholder prepares OI and PI and constructs the dual signature
  - Transaction ID included in both
- PI is symmetrically encrypted, encryption key is encrypted with Gateway’s public key
- **Purchase Request** – Cardholder sends own certificate, dual signature, encrypted PI, PI digest and OI
- Merchant checks signature
- If all is ok, **Purchase Response** is sent



1. Initiate Request
2. Initiate Response
3. Purchase Request
6. PurchaseResponse

Payment Authorization

- **Authorization Request** – Merchant sends
  - Encrypted PI, dual signature, OI digest, Signed Transaction ID, Cardholder’s and Merchant’s Certificates
- Everything is signed by merchant and symmetrically encrypted, encryption key is encrypted with Gateway’s public key
- Gateway verifies certificates and signatures and checks that transaction ID is same in PI and message.
- Gateway authorizes payment with issuing bank
- **Authorization Response** – Response that purchase is authorized is returned to merchant, symmetrically encrypted, encryption key is encrypted with Merchant’s public key
- **Capture request and response** – Payment is finalized



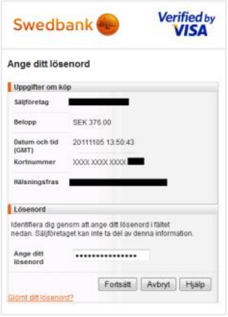
1. Initiate Request
2. Initiate Response
3. Purchase Request
6. PurchaseResponse
4. Authorization Request
5. Authorization Response
7. Capture Request
8. Capture Response

What happened to SET?

- Technically great
  - Confidentiality, authentication, integrity and non-repudiation on message level
- Merchant does not get the card details
- Some reasons for failure:
  - Cardholder needed to install special software on PC
    - Possibly creating interoperability problems
    - Problem with malware
  - Not very simple for users with limited computer skills
  - PKI infrastructure needed
  - Complex scheme with large deployment costs

3D Secure

- New attempt to secure online purchases
  - Developed by Visa and adopted also by MasterCard
- Very different from SET
- Cardholder is authenticated with issuer
  - Verify that she owns the card
  - The rest is ”as usual”
- Three Domains (the 3D in the name)
  - Issuer domain – The cardholder and the issuing bank
  - Acquirer domain – The Merchant and the acquiring bank
  - Interoperability domain – Domain connecting issuing and acquiring domain (card network and Internet)



Swedbank

Verified by VISA

Ange ditt lösenord

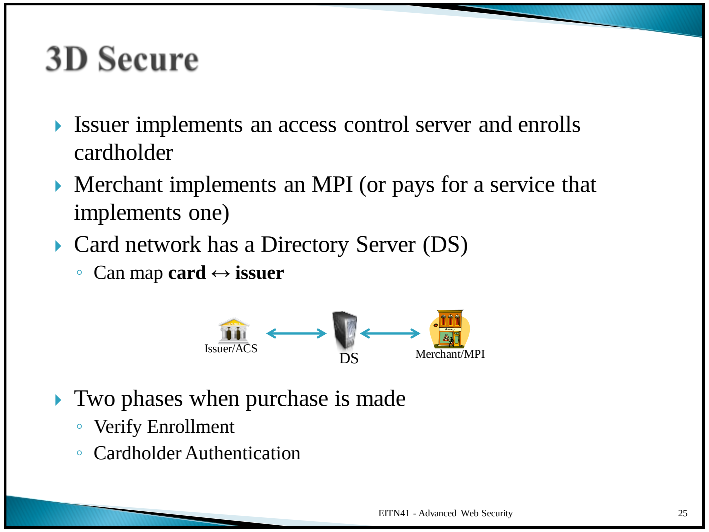
Uppgifter om köp

Säljföretag	[redacted]
Belopp	SEK 376.00
Datum och tid (GMT)	20111105 13:50:43
Kortnummer	XXXX XXXX XXXX [redacted]
Hälsningsfras	[redacted]

Lösenord

Identifiera dig genom att ange ditt lösenord i fältet nedan. Säljföretaget kan inte ta del av denna information.

Ange ditt lösenord ••••••••••••••••

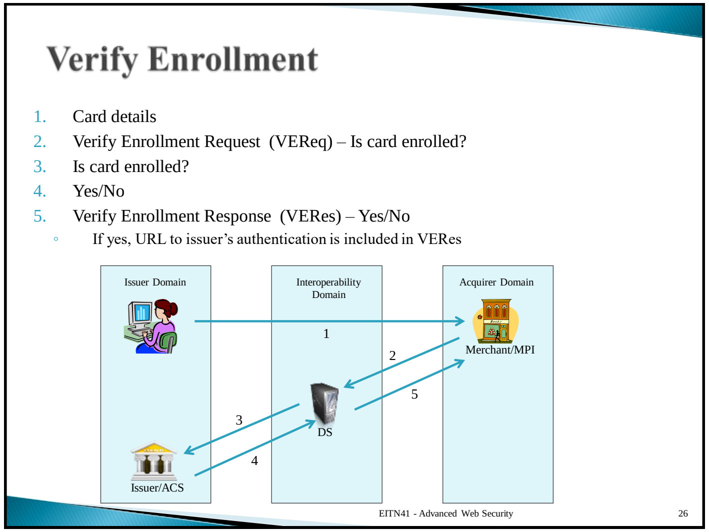


3D Secure

- Issuer implements an access control server and enrolls cardholder
- Merchant implements an MPI (or pays for a service that implements one)
- Card network has a Directory Server (DS)
  - Can map **card** ↔ **issuer**

Issuer/ACS
DS
Merchant/MPI

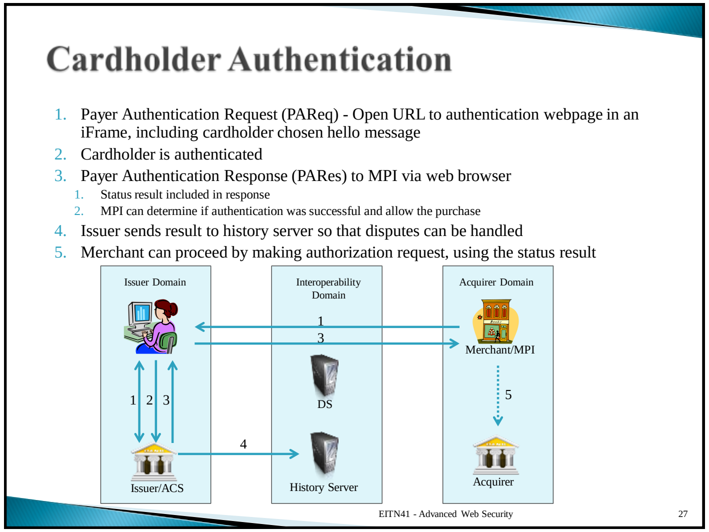
- Two phases when purchase is made
  - Verify Enrollment
  - Cardholder Authentication



Verify Enrollment

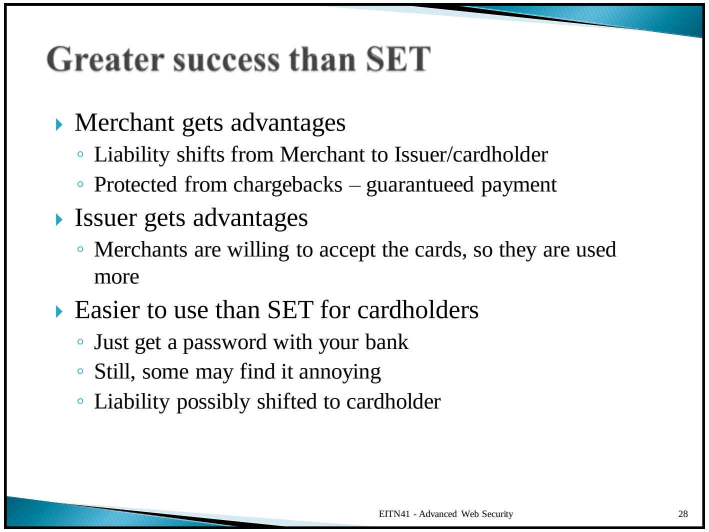
1. Card details
2. Verify Enrollment Request (VEReq) – Is card enrolled?
3. Is card enrolled?
4. Yes/No
5. Verify Enrollment Response (VERes) – Yes/No
   - If yes, URL to issuer's authentication is included in VERes

Issuer Domain
Interoperability Domain
Acquirer Domain
1
Merchant/MPI
2
5
3
DS
4
Issuer/ACS



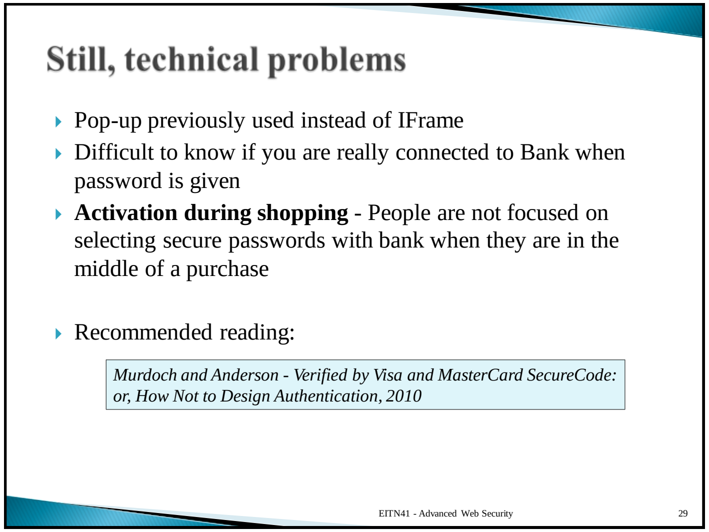
Cardholder Authentication

1. Payer Authentication Request (PAReq) - Open URL to authentication webpage in an iFrame, including cardholder chosen hello message
2. Cardholder is authenticated
3. Payer Authentication Response (PARes) to MPI via web browser
   1. Status result included in response
   2. MPI can determine if authentication was successful and allow the purchase
4. Issuer sends result to history server so that disputes can be handled
5. Merchant can proceed by making authorization request, using the status result



Greater success than SET

- Merchant gets advantages
  - Liability shifts from Merchant to Issuer/cardholder
  - Protected from chargebacks – guarantueed payment
- Issuer gets advantages
  - Merchants are willing to accept the cards, so they are used more
- Easier to use than SET for cardholders
  - Just get a password with your bank
  - Still, some may find it annoying
  - Liability possibly shifted to cardholder

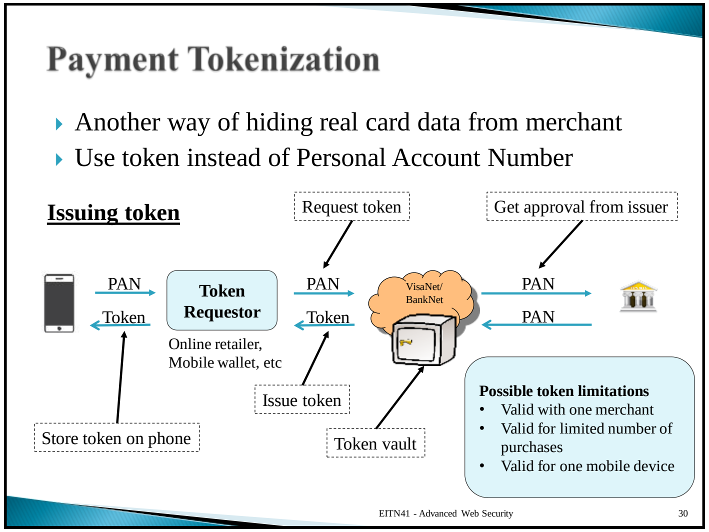


Still, technical problems

- Pop-up previously used instead of IFrame
- Difficult to know if you are really connected to Bank when password is given
- **Activation during shopping** - People are not focused on selecting secure passwords with bank when they are in the middle of a purchase

- Recommended reading:

Murdoch and Anderson - Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication, 2010



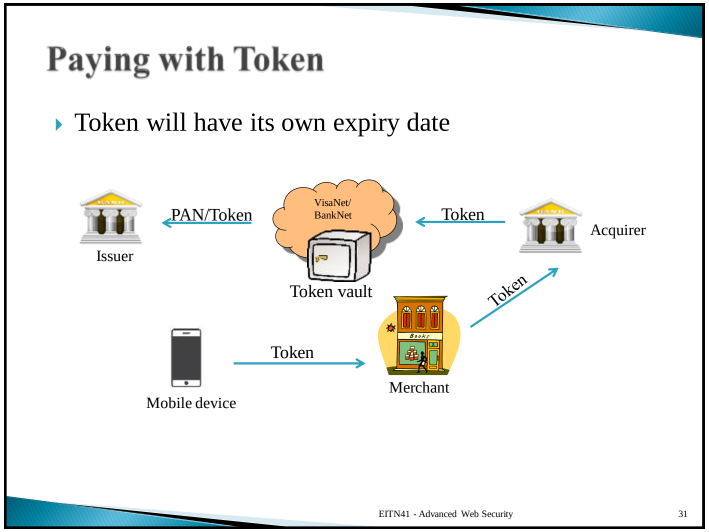
Payment Tokenization

- Another way of hiding real card data from merchant
- Use token instead of Personal Account Number

Issuing token

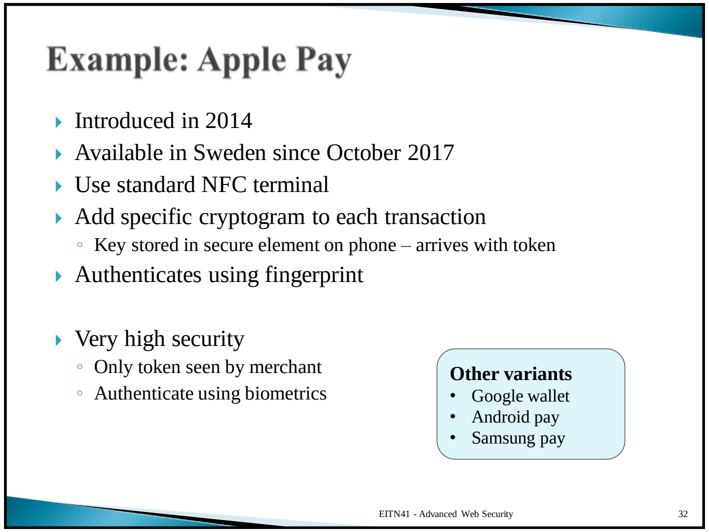
Possible token limitations

- Valid with one merchant
- Valid for limited number of purchases
- Valid for one mobile device



Paying with Token

- Token will have its own expiry date



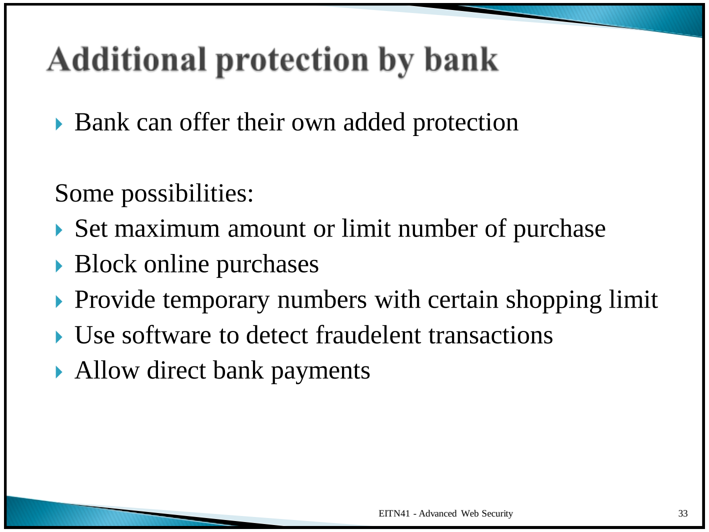
Example: Apple Pay

- Introduced in 2014
- Available in Sweden since October 2017
- Use standard NFC terminal
- Add specific cryptogram to each transaction
  - Key stored in secure element on phone – arrives with token
- Authenticates using fingerprint

- Very high security
  - Only token seen by merchant
  - Authenticate using biometrics

Other variants

- Google wallet
- Android pay
- Samsung pay



Additional protection by bank

- Bank can offer their own added protection

Some possibilities:

- Set maximum amount or limit number of purchase
- Block online purchases
- Provide temporary numbers with certain shopping limit
- Use software to detect fraudelent transactions
- Allow direct bank payments