# Introduction to Digital Signatures, PKI, and Certificates

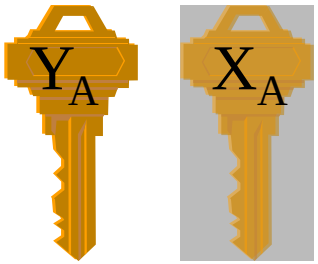
Vigil Security LLC

Russ Housley

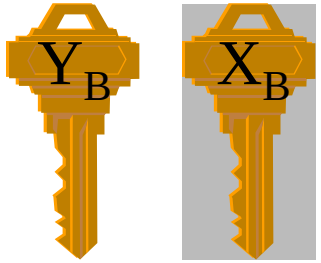
4 December 2018

# Motivation

- STIR / SHAKEN depends upon digital signatures, Public Key Infrastructure (PKI), and certificates
- This session provides a basic introduction to theses technologies
- Hopefully, this introduction will provide a firm foundation for the talks that come later in the day




# Public Key Cryptography




- Every party has a key pair:
  a *private key* and a *public key*
  - The private and public keys are mathematically related, but it is computationally infeasible to determine the private key from the public key
  - The private key is never shared; it must be well protected
  - The public key is freely distributed, typically in a certificate

# Public Key 101

- An certification authority (CA) builds a certificate that includes:
  - Subject's Name
  - Subject's Public Key
  - Issuer's Name
  - Validity Period
  - Other data to help manage certificates


- The issuer *digitally signs* the certificate
  - Any change to the content can be detected

# Digitized vs. Digital Signature

- A *digitized signature* is a scanned image that can be pasted into a document
- A *digital signature* is a value that is created with the signer's private key; it can be validated by anyone with the signer's public key

***Digitized*** Signature

```
7A606F666BCC65F9720BC07F8
E52C7D25866B71DD640713242
64A75AA53F09D002200F14D7F
E21F0496B1F7E6B8F8A750DFA
BD34A3946F6297AB2730966BB
```

***Digital*** Signature

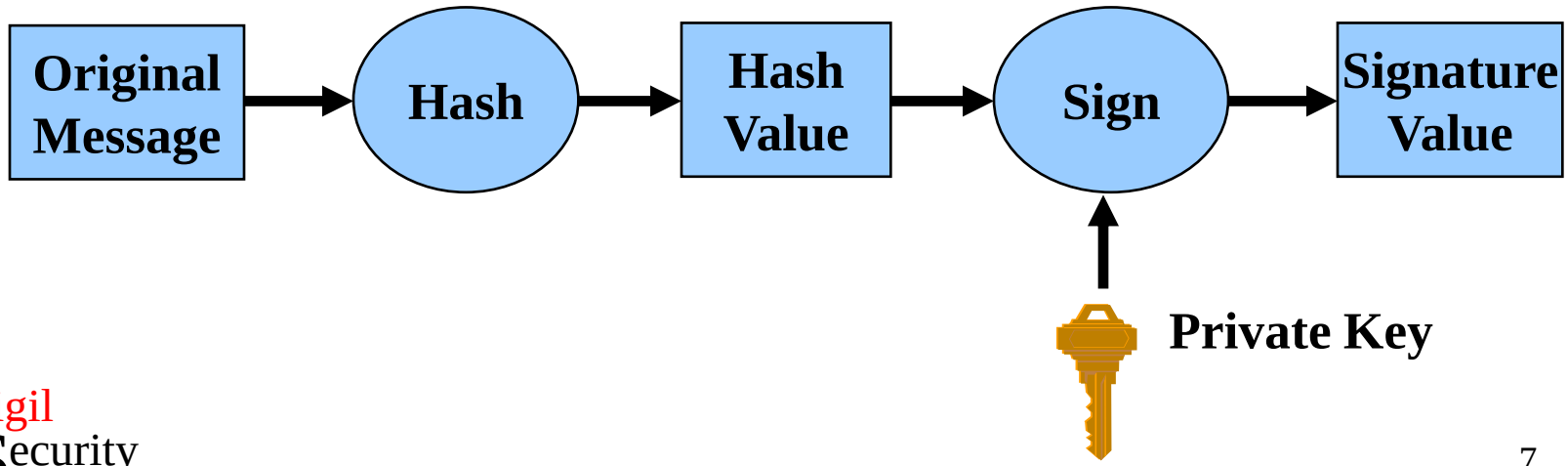
Vigil Security LLC

# Hash Functions

- One way functions provide integrity
- Provide a single hash value with a uniform size for any length message
- Computationally infeasible to:
  - Derive the original message from the hash value
  - Create a second message with the same hash value the original message

# Digital Signing

- A one-way hash function is used to create a hash of the data to be signed
- A digital signature is the output from a cryptographic transformation of the hash value using the signer's *private* key



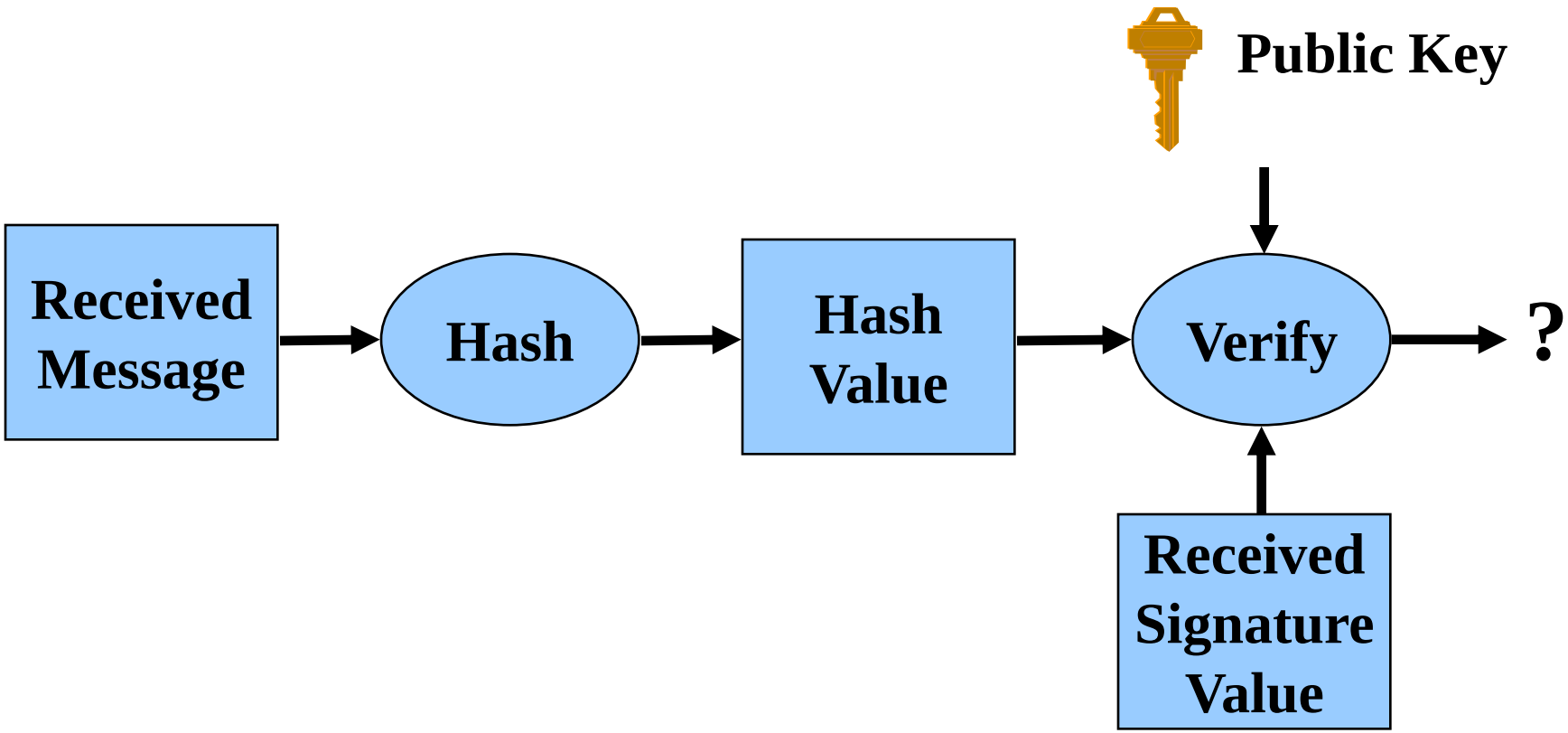
# STIR Environment

- A PASSporT (Personal Assertion Token) is the protocol data object that is signed
- Digital Signature Algorithms:
  - ECDSA using P-256 with SHA-256
  - RSA with SHA-256
- STIR PASSporT is always signed with ECDSA
- STIR Certificate signed with ECDSA or RSA

# Verification

- The STIR PASSporT and the digital signature value are sent to the recipient
- The recipient hashes the data and the uses the sender's public key to check the signature
  - Certificate holds the public key
  - Certificate can be cached to reduce size
- The verification will pass or fail

# Digital Signature Verification



# Certification Authority

- Generates and digitally signs the certificate
  - Binds Subject's name to public key
- Revokes certificate if information changes
- Revokes certificate if private key is disclosed
- Support certificate hierarchies

# Certificate Policy

- The rules and requirements for security, trust, and assurance
- A named set of rules that indicate whether a certificate meets the security requirements of a particular community or application
- Provides the foundation for audit
- In short: *What* the CA does

# Certification Practice Statement

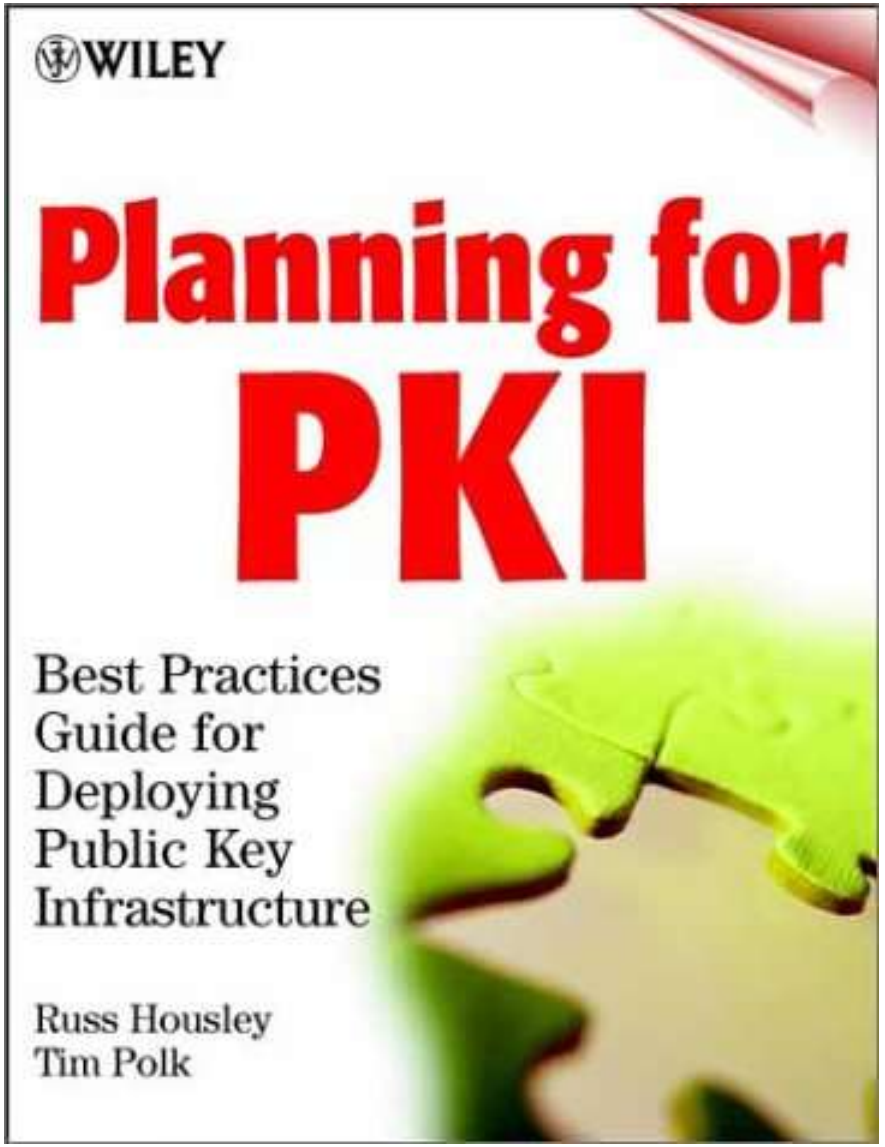
- A statement of the practices, which a CA employs in issuing certificates
- Compliance audit of CPS to CP is recognized as vehicle for trust in a CA
- In short: *How* the CA does its job

# References

- RFC 5280: Certificates
- RFC 8226: STIR Certificate Profile
- RFC 3647: CP and CPS Framework
- RFC 8225: PASSporT

# For More Information

**Russ Housley**
housley@vigilsec.com
+1 703 435 1775




Vigil Security LLC