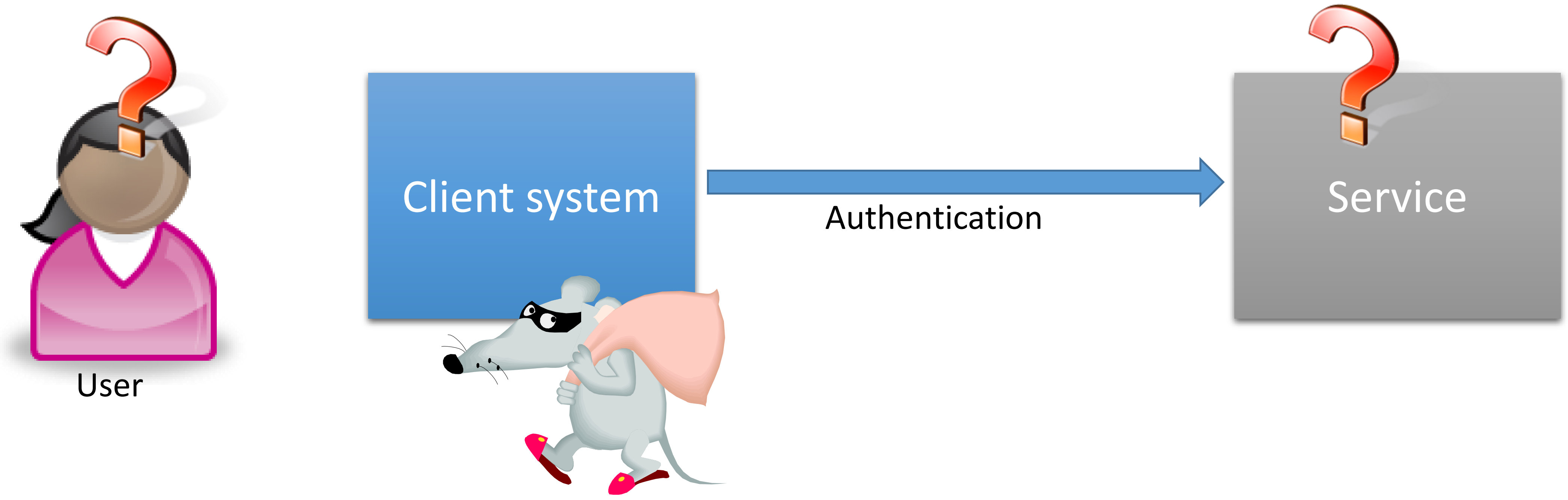
Improving Trusted Tickets with State-Bound Keys

Jan Nordholz, TU Berlin

Ronald Aigner, Microsoft Research

The problem



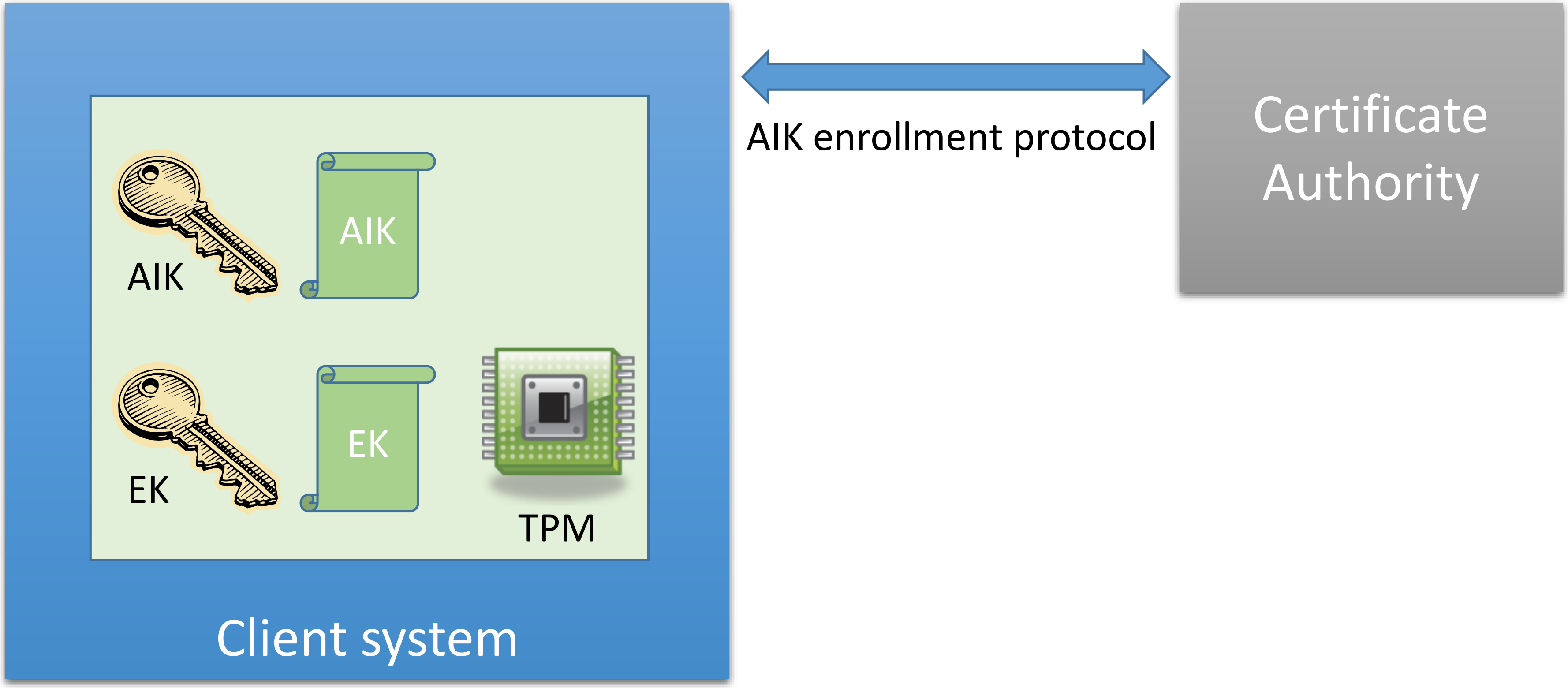
Can user **trust PC** to represent her correctly?

Can service **trust PC** to represent user?

Outline

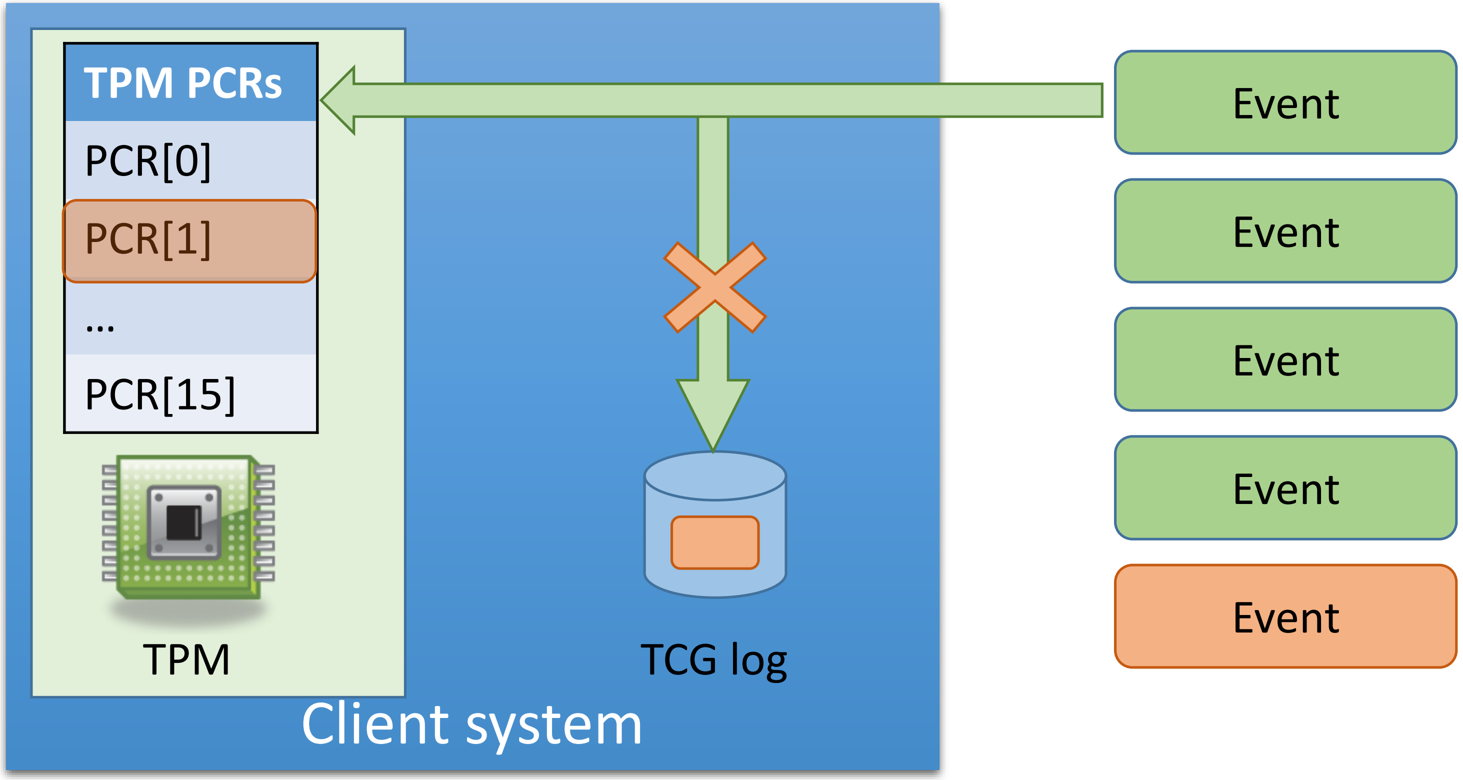
- TPM based attestation background
- Keeping it fresh
- Kerberos network authentication background
- Adding machine health state to Kerberos
- Evaluation & Conclusion

TPM attestation background



Trust EK certificate → Trust EK → Trust AIK → AIK certificate

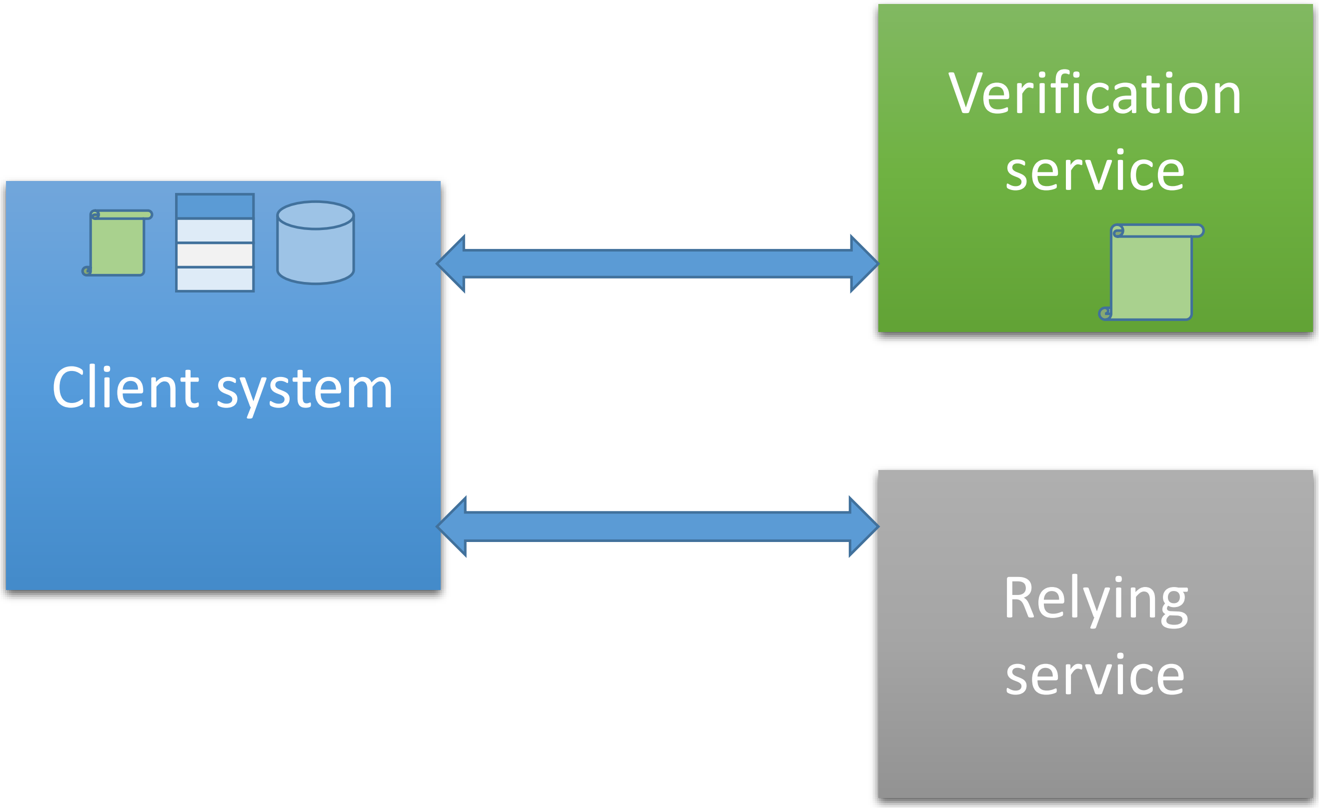
TPM attestation background (contd.)



AIK certificate → Trust in AIK → Trust in PCRs → Trust in TCG log

TPM attestation background (contd.)

- Collect state of system



- Check cryptographic keys
- Verify system state
- Provide health statement

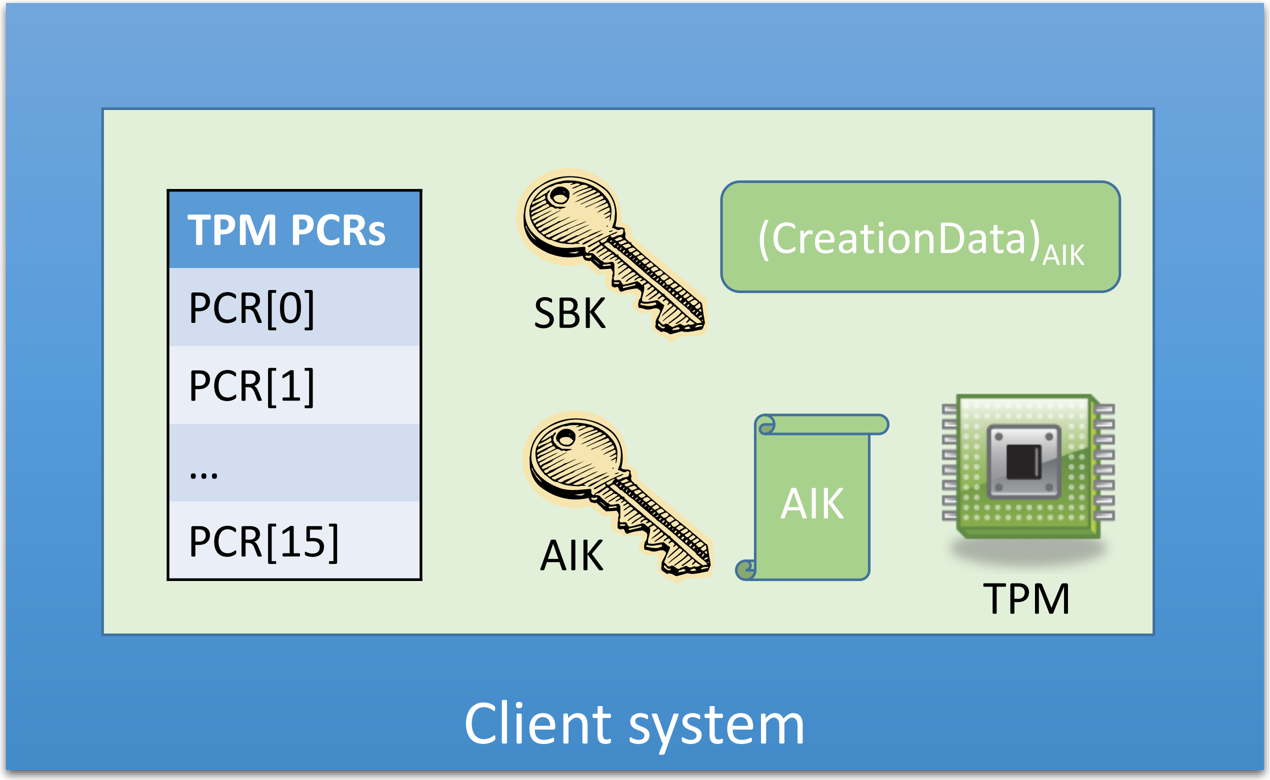
- Check health statement

Trust in AIK → Trust in PCRs → Trust in TCG log → Health Statement

Outline

- TPM based attestation background
- Keeping it fresh
- Kerberos network authentication background
- Adding machine health state to Kerberos
- Evaluation & Conclusion

State bound keys

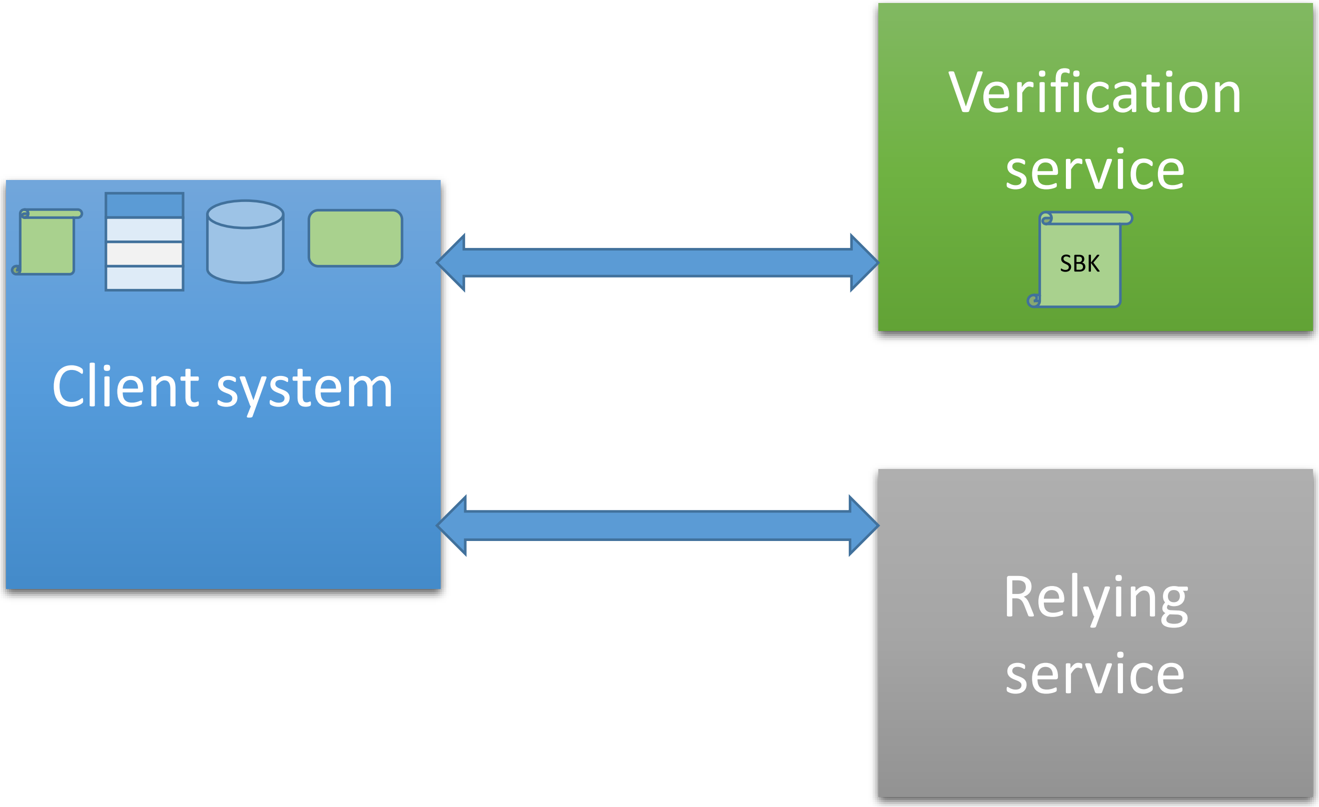


TPM PCRs
PCR[0]
PCR[1]
…
PCR[15]

TPM keys can be bound to PCRs – Only work when PCRs stay the same

TPM attestation with SBK

- Collect state of system

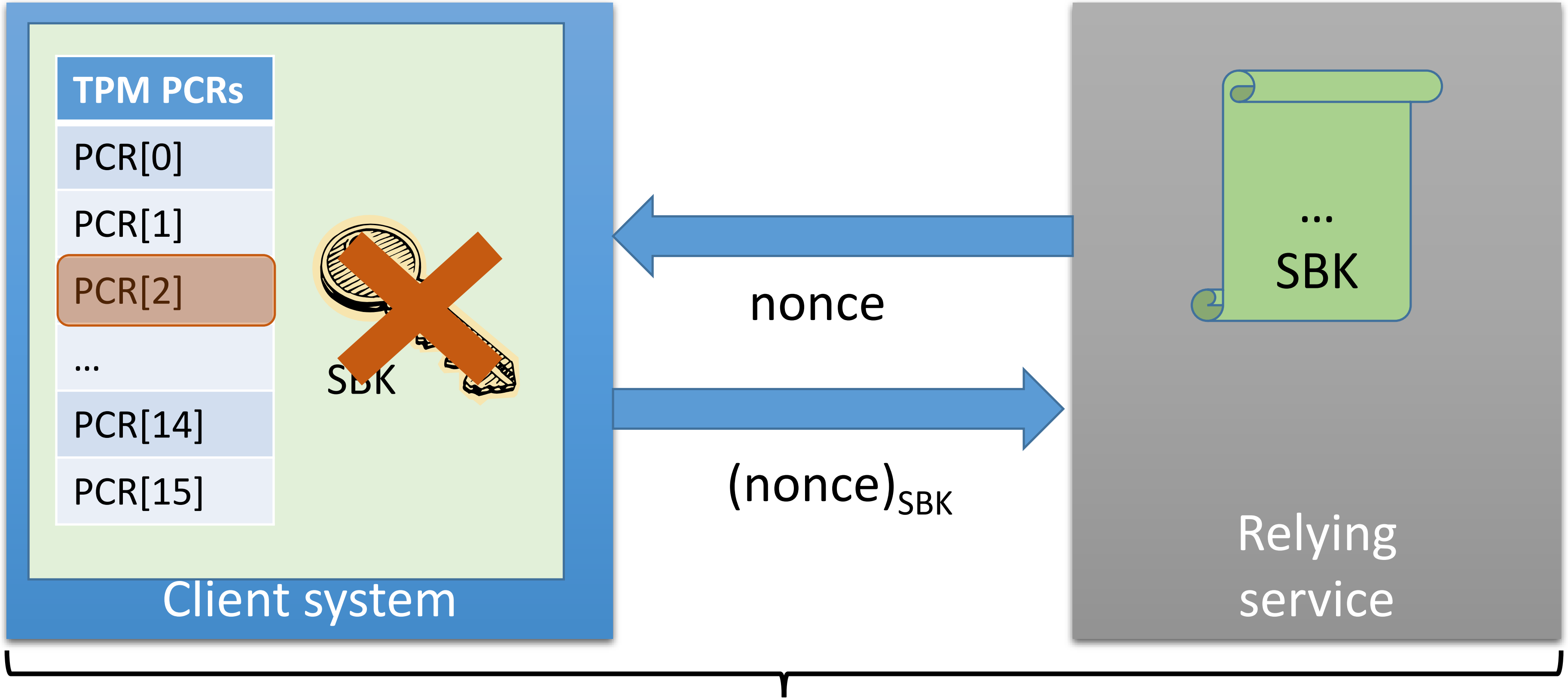


- Check cryptographic keys
- Verify system state
- Provide health statement

- Check health statement

Trust in AIK → Trust in PCRs → Trust in TCG log → Health Statement + SBK

Challenging state bound keys



TPM PCRs

PCR[0]

PCR[1]

PCR[2]

…

PCR[14]

PCR[15]

SBK

Client system

nonce

(nonce)$_{SBK}$

…

SBK

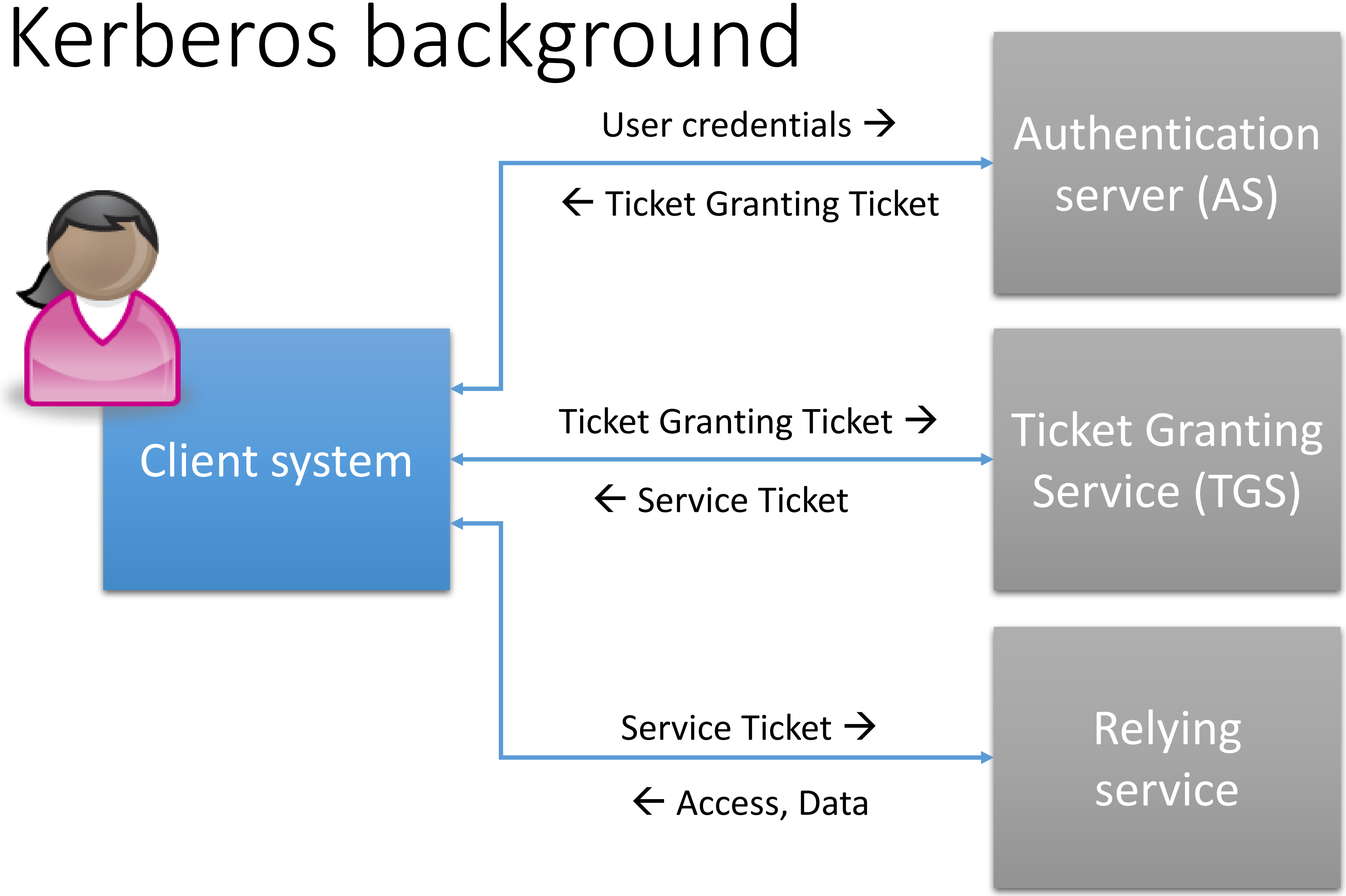
Relying service

SBK proof

Outline

- TPM based attestation background
- Keeping it fresh
- Kerberos network authentication background
- Adding machine health state to Kerberos
- Evaluation & Conclusion

Kerberos background



User credentials →

← Ticket Granting Ticket

Authentication server (AS)

Client system

Ticket Granting Ticket →

← Service Ticket

Ticket Granting Service (TGS)

Service Ticket →

← Access, Data

Relying service

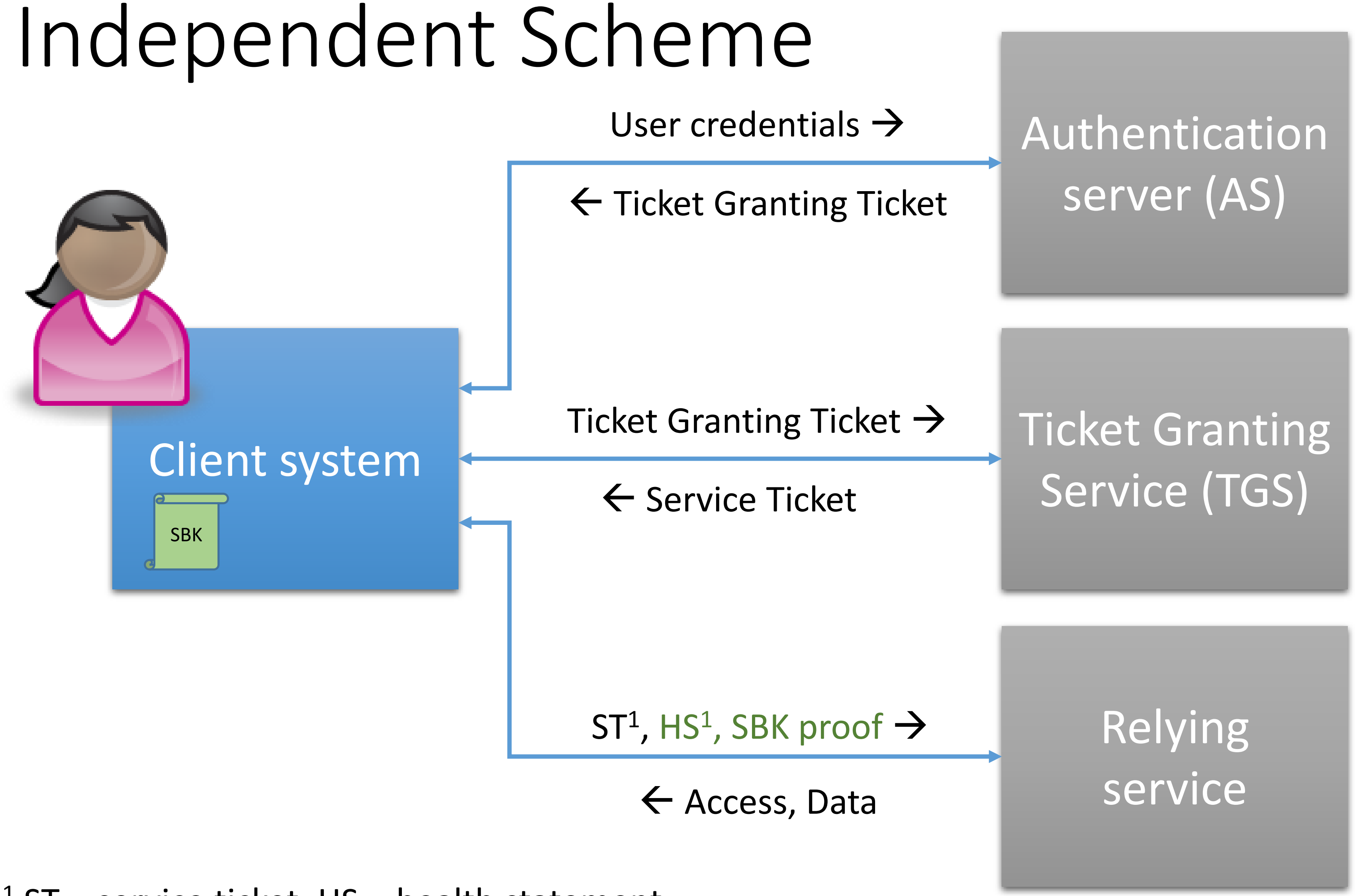
TGT has long lifetime
(once per log on)

Service ticket has
shorter lifetime

Outline

- TPM based attestation background
- Keeping it fresh
- Kerberos network authentication background
- Adding machine health state to Kerberos
- Evaluation & Conclusion

Independent Scheme

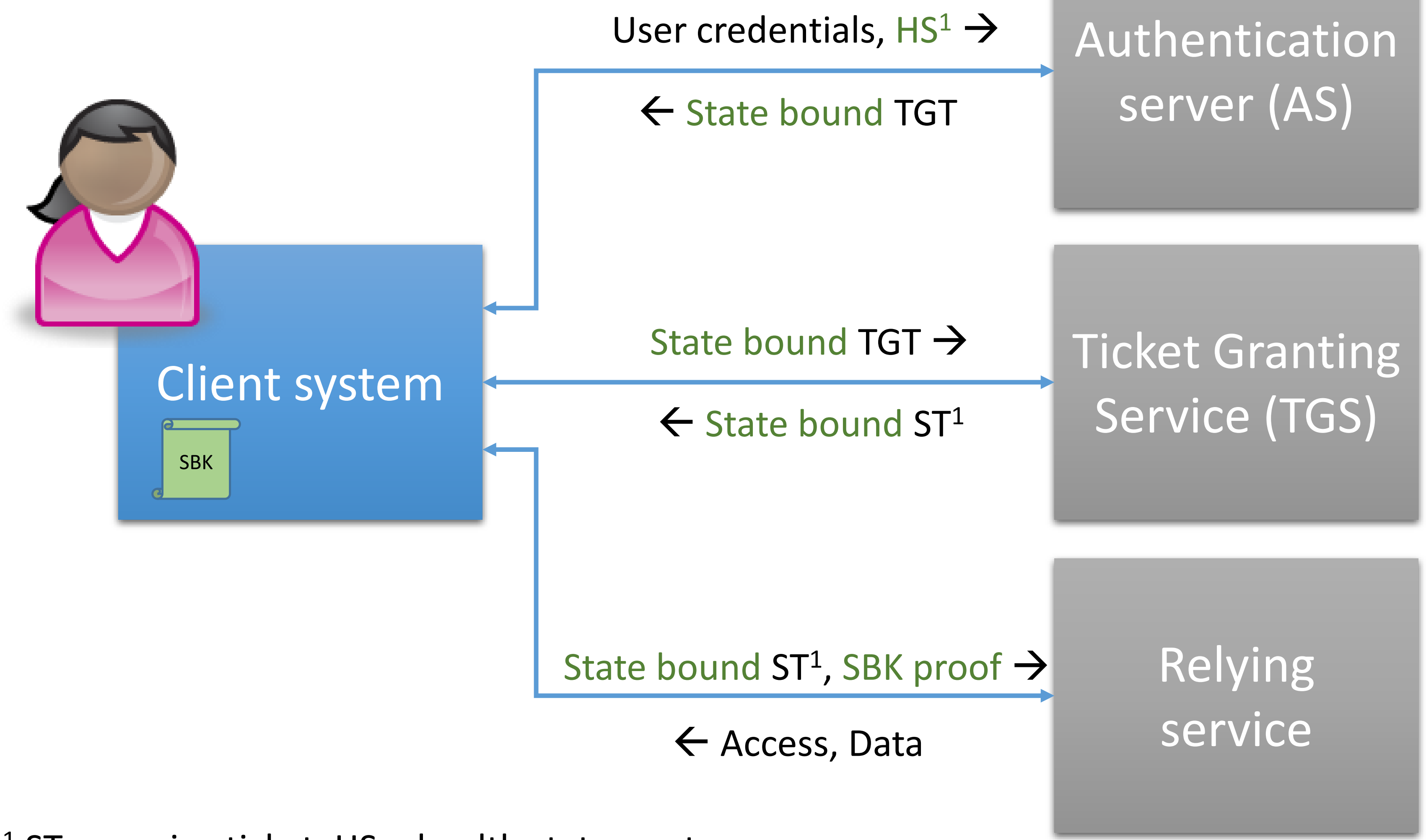


➕ No AS and TGS involvement

➖ Evaluation burden on service

[1] ST – service ticket, HS – health statement

Early check scheme



User credentials, HS[1] →

← State bound TGT

Authentication server (AS)

Client system

SBK

State bound TGT →

← State bound ST[1]

Ticket Granting Service (TGS)

State bound ST[1], SBK proof →

← Access, Data

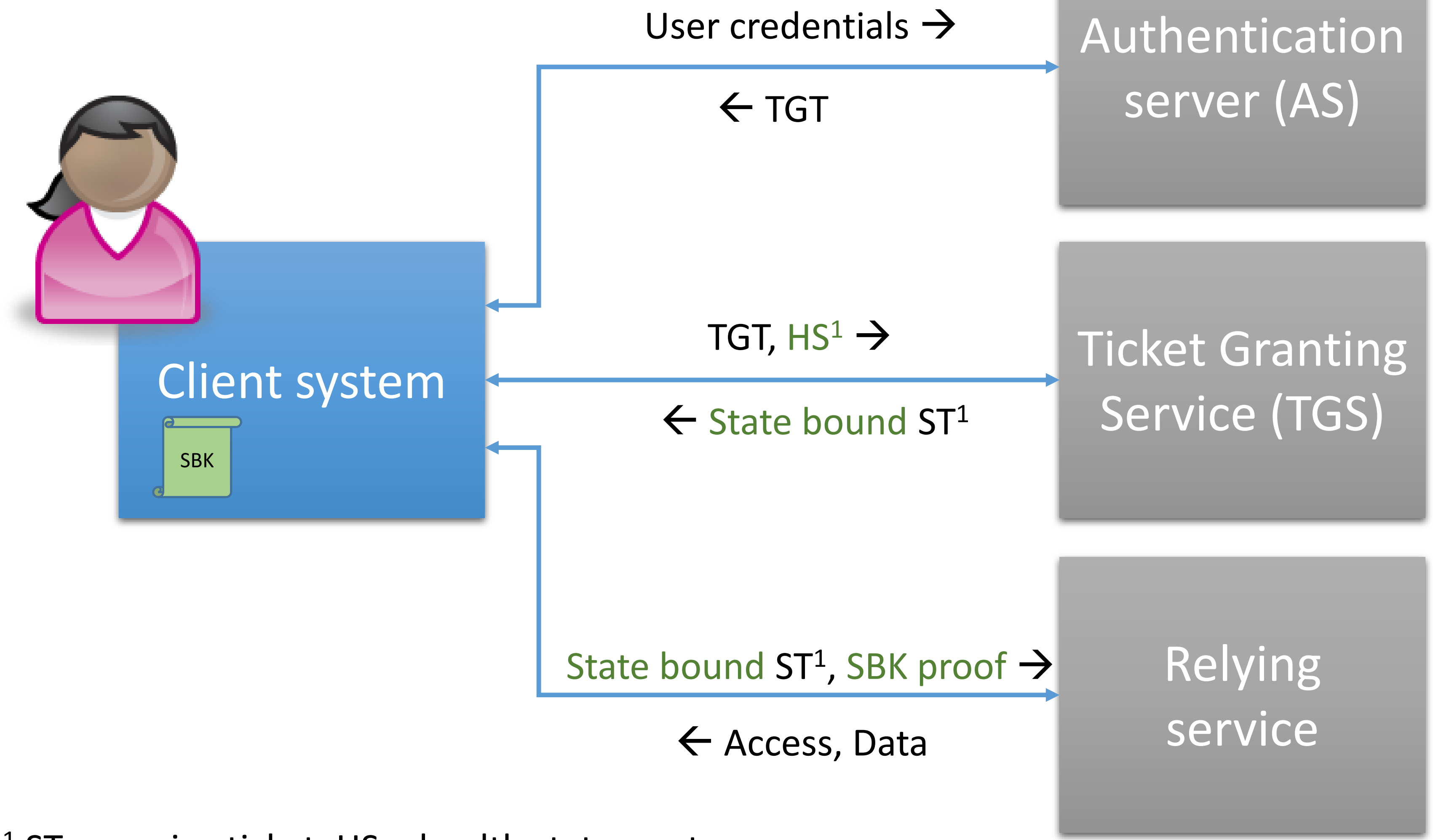
Relying service

− Breaks Kerberos Single Sign-On

+ Little work for actual service

[1] ST – service ticket, HS – health statement

Intermediate Scheme



User credentials →

← TGT

TGT, HS[1] →

← State bound ST[1]

State bound ST[1], SBK proof →

← Access, Data

Client system

SBK

Authentication server (AS)

Ticket Granting Service (TGS)

Relying service

✚ Keeps Kerberos SSO intact

✚ Some evaluation load in TGS

✚ Little work for actual service

[1] ST – service ticket, HS – health statement

Conclusion

- Using state bound keys allows to verify validity of health statement.
- No longer need to attest periodically.
- Can be integrated in different client – service scenarios.

- Service and User can trust client machine to behave properly.

Q & A

- Thank you