Integrität und Vertraulichkeit

KISTERS
Mit der Kompetenz der Pioniere.

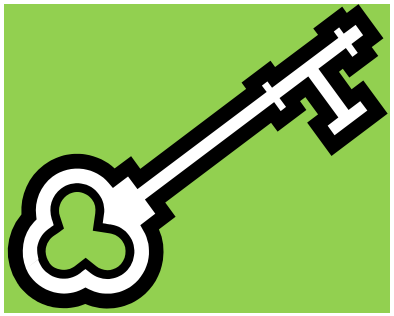
Integrität

KISTERS
Mit der Kompetenz der Pioniere.

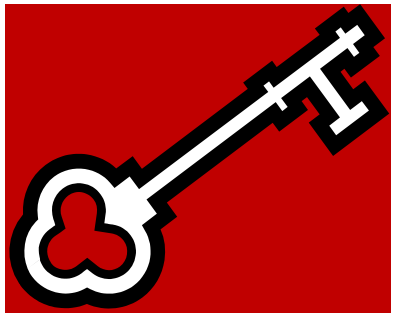
Integrität

- Signierung der Nachricht
- Ein privater, ein öffentlicher Schlüssel
- NSW-Kernsystem kann die Signatur überprüfen
- Gleiches Zertifikat wie beim Zugriff auf das NSW (Evaluierung)

Institution



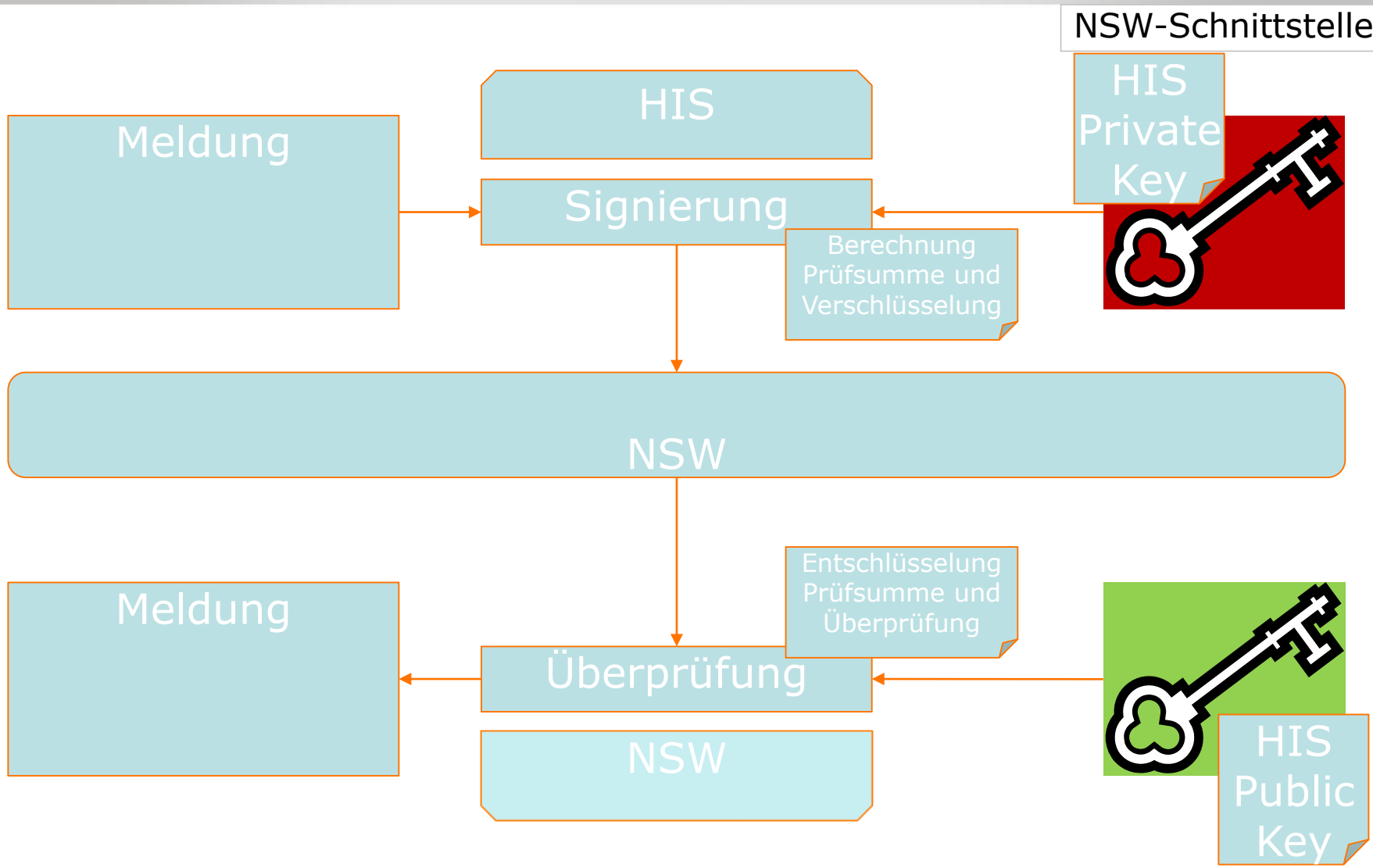
Öffentlicher Schlüssel



Privater Schlüssel

KISTERS

Integrität



KISTERS

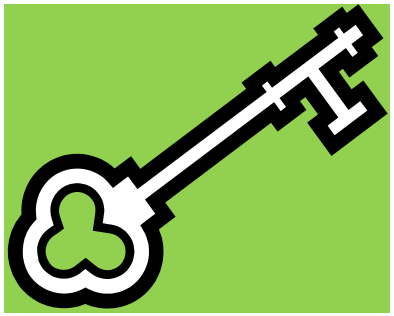
Vertraulichkeit

KISTERS
Mit der Kompetenz der Pioniere.

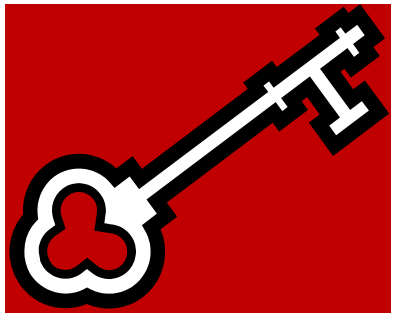
Vertraulichkeit

- Verschlüsselung von Teilen der Meldung
- Ein privater, ein öffentlicher Schlüssel
- NSW-Kernsystem kann keine Entschlüsselung vornehmen

Institution



Öffentlicher Schlüssel

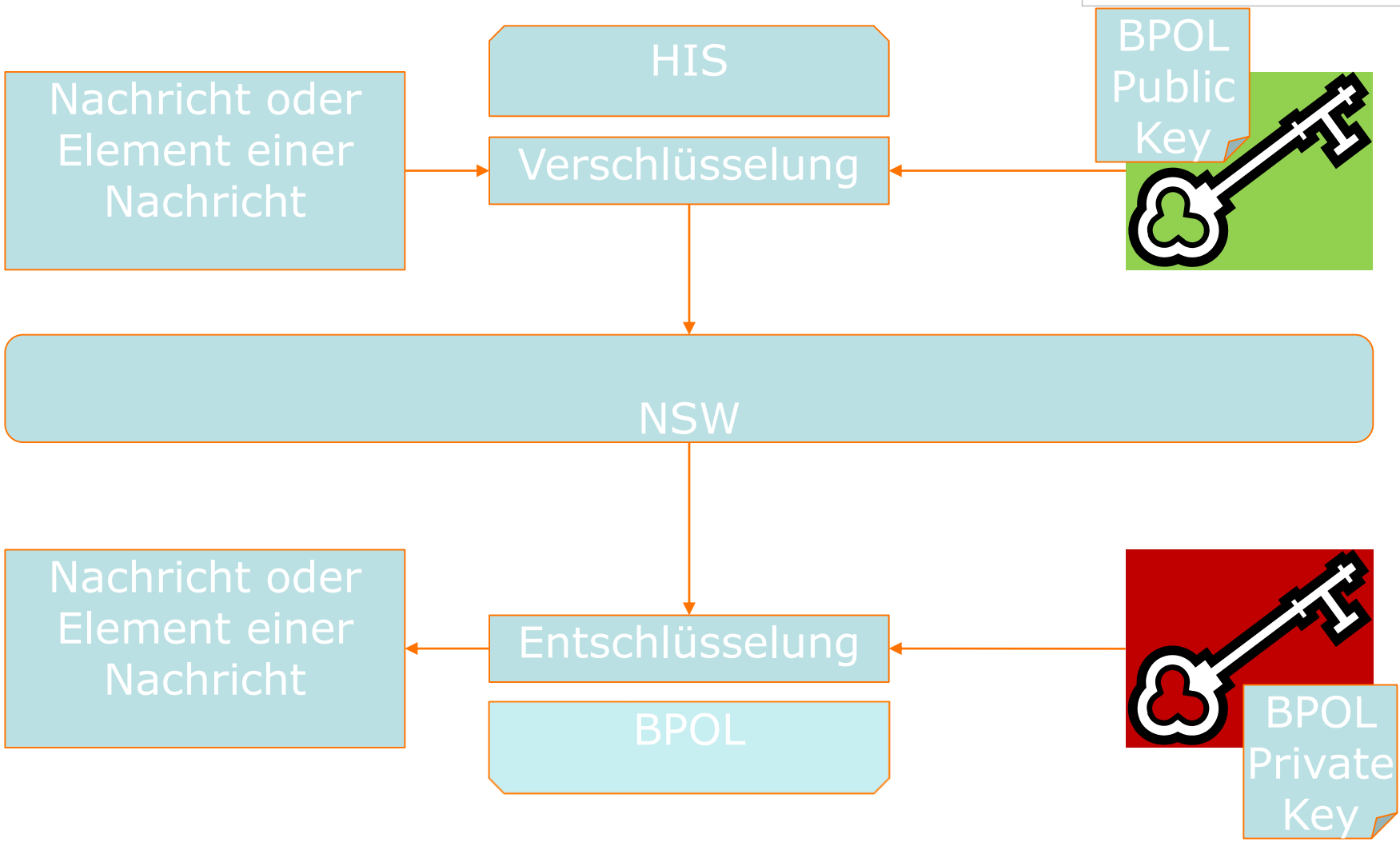


Privater Schlüssel

KISTERS

Vertraulichkeit

NSW-Schnittstelle



KISTERS

Vertraulichkeit (Alternative)

- Verschlüsselung von Elementinhalten mit AES-256
- Ein synchroner Schlüssel
- Schlüsselaustausch direkt zwischen Institutionen

KISTERS

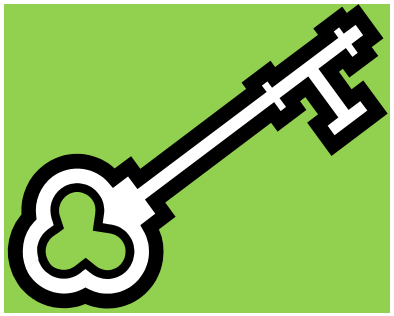
Eingesetzte Technologie

KISTERS
Mit der Kompetenz der Pioniere.

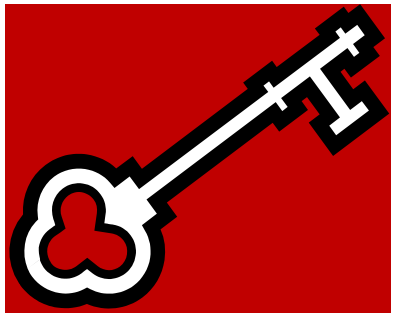
Technologie

- WS-Security
- Aufsatz zu SOAP-WebServices
- Hohe Wertigkeit der Signierung / Verschlüsselung
- Zu klärender Punkt: Schlüsselaustausch

Institution



Öffentlicher Schlüssel



Privater Schlüssel

Vielen Dank für Ihre Aufmerksamkeit!

KISTERS
Mit der Kompetenz der Pioniere.