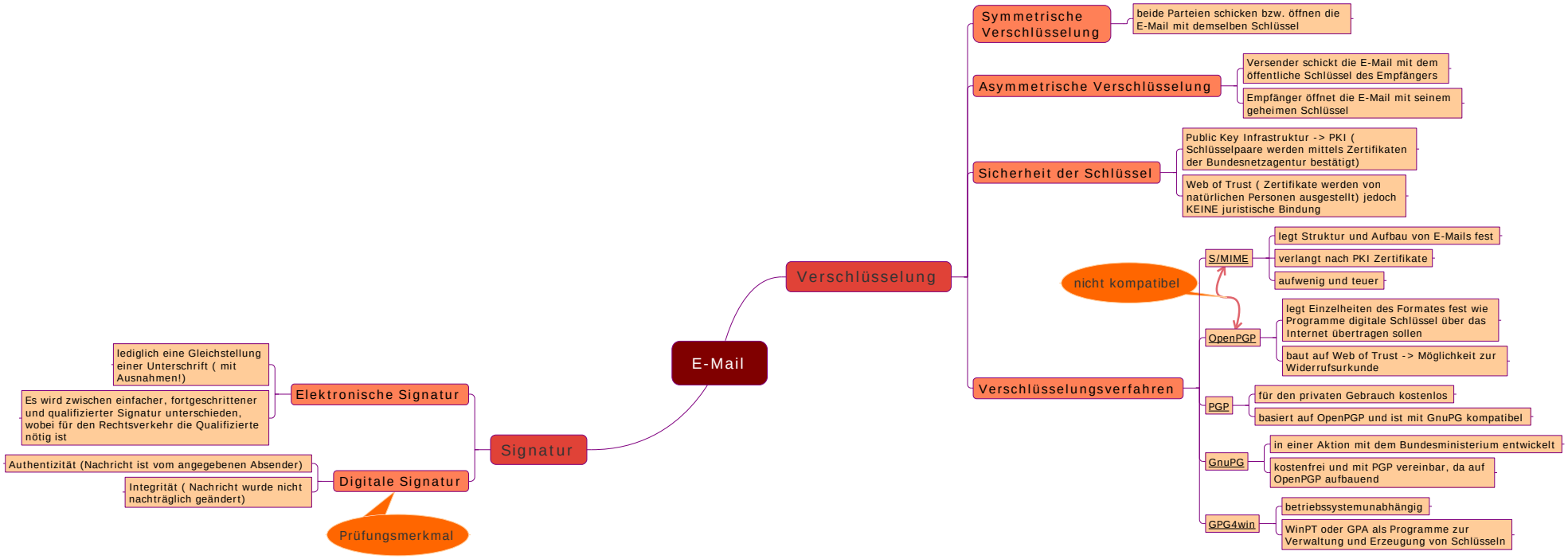
E-Mail
Verschlüsselung
Symmetrische Verschlüsselung
beide Parteien schicken bzw. öffnen die E-Mail mit demselben Schlüssel
Asymmetrische Verschlüsselung
Versender schickt die E-Mail mit dem öffentliche Schlüssel des Empfängers
Empfänger öffnet die E-Mail mit seinem geheimen Schlüssel
Sicherheit der Schlüssel
Public Key Infrastruktur -> PKI (Schlüsselpaare werden mittels Zertifikaten der Bundesnetzagentur bestätigt)
Web of Trust (Zertifikate werden von natürlichen Personen ausgestellt) jedoch KEINE juristische Bindung
Verschlüsselungsverfahren
nicht kompatibel
S/MIME
legt Struktur und Aufbau von E-Mails fest
verlangt nach PKI Zertifikate
aufwenig und teuer
OpenPGP
legt Einzelheiten des Formates fest wie Programme digitale Schlüssel über das Internet übertragen sollen
baut auf Web of Trust -> Möglichkeit zur Widerrufsurkunde
PGP
für den privaten Gebrauch kostenlos
basiert auf OpenPGP und ist mit GnuPG kompatibel
GnuPG
in einer Aktion mit dem Bundesministerium entwickelt
kostenfrei und mit PGP vereinbar, da auf OpenPGP aufbauend
GPG4win
betriebssystemunabhängig
WinPT oder GPA als Programme zur Verwaltung und Erzeugung von Schlüsseln
Signatur
Elektronische Signatur
lediglich eine Gleichstellung einer Unterschrift (mit Ausnahmen!)
Es wird zwischen einfacher, fortgeschrittener und qualifizierter Signatur unterschieden, wobei für den Rechtsverkehr die Qualifizierte nötig ist
Digitale Signatur
Authentizität (Nachricht ist vom angegebenen Absender)
Integrität (Nachricht wurde nicht nachträglich geändert)
Prüfungsmerkmal