TeleTrusT EBCA
European Bridge Certificate Authority

TeleTrusT-EBCA "PKI-Workshop"

Berlin, 26.06.2018

Lieber eine schlechte Verschlüsselung als keine, oder?

Sören Beiler, Net at Work GmbH

Net at Work
Building IT-Excellence.

Cipher Suites im Vergleich

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_ECDHE_ECDSA_ AES_256_GCM_SHA384

Protokoll für die Cipher Suite (TLS, SSL)

Key Exchange

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

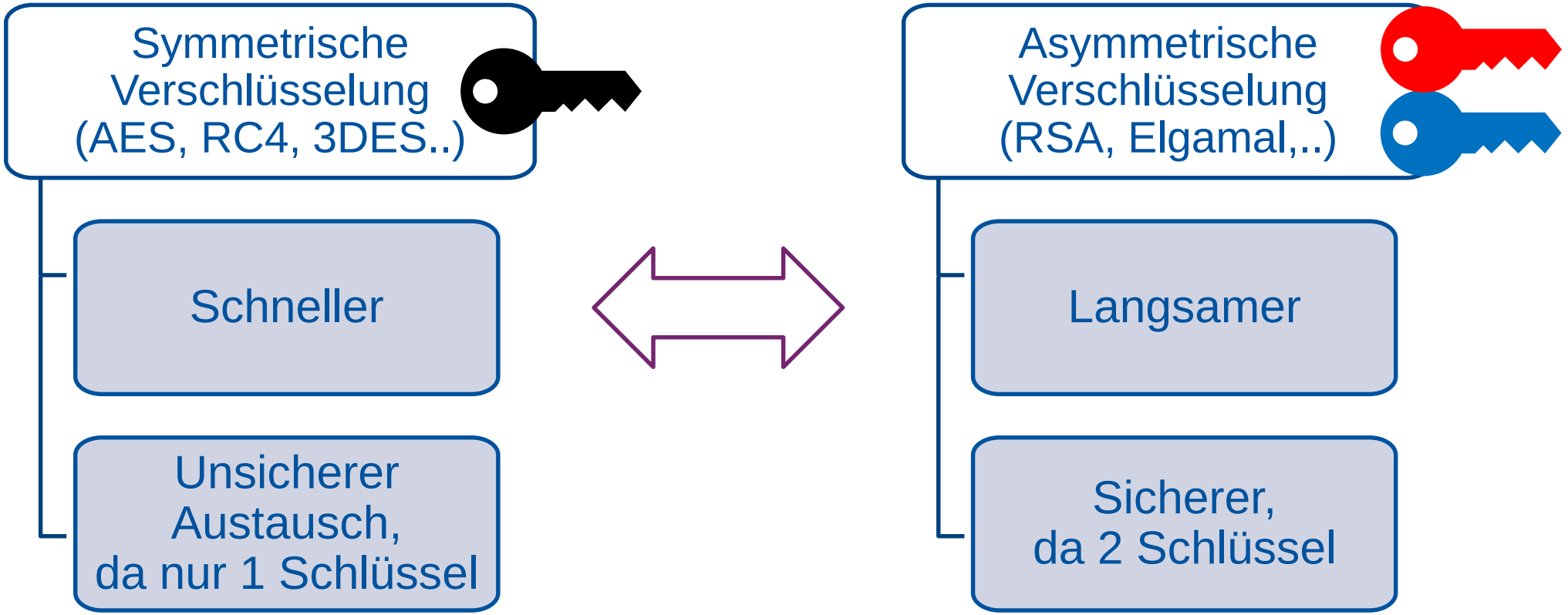
Block Cipher

Message Authentication

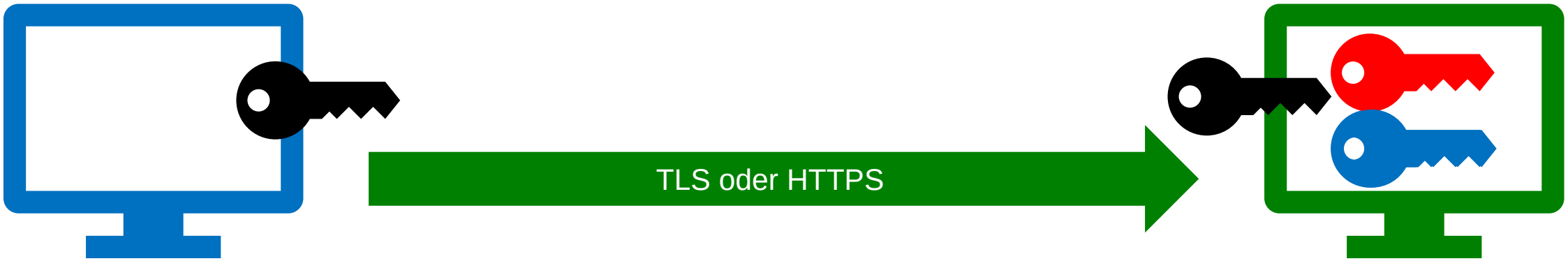
Protokolle

- SSL v3
  - Veröffentlichung 1996
  - Abgekündigt seit Juni 2015 (POODLE)
- TLS 1.0
  - Veröffentlichung 1999
  - Empfehlung für Update vor Juli 2018
- TLS 1.1
  - Veröffentlichung 2006
  - Besserer Schutz vor CBC Attacken
- TLS 1.2
  - Veröffentlichung 2008
  - Einführung von Authenticated Encryption

Key Exchange



Key Exchange



Key Exchange

RSA	• Schlüsselgenerierung mit RSA
DH	• Diffie Hellmann
DHE	• Ephemeral Diffie Hellmann
ECDH	• Elliptic curve DH
ECDHE	• Ephemeral Elliptic curve DH
PSK	• Pre-shared Secret

FORWARD SECRECY

Key Exchange

Schlüsselaustausch/Agreement mittels ECDHE Mit PFS!

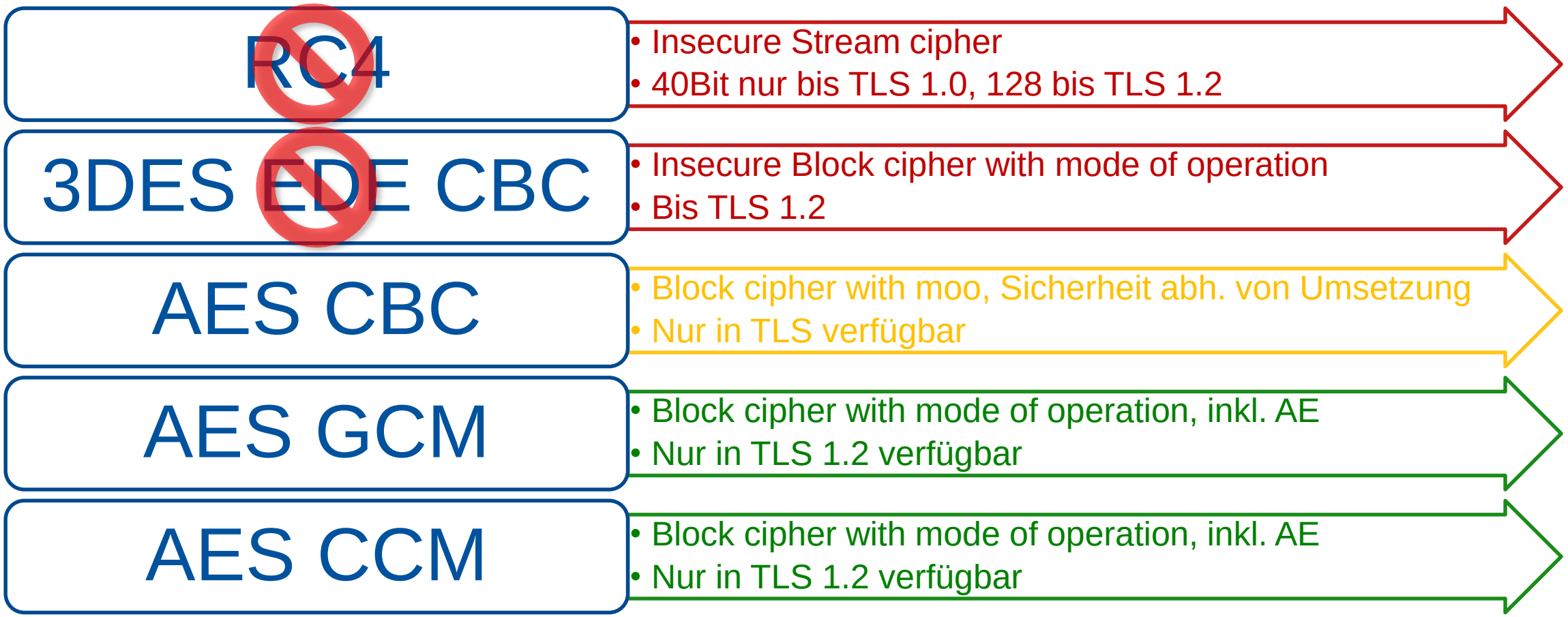
Schlüssel ist signiert!

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_3DES_EDE_CBC_SHA

Schlüsselaustausch mittels RSA
Kein PFS, keine Signatur.

Block Cipher



Block Cipher

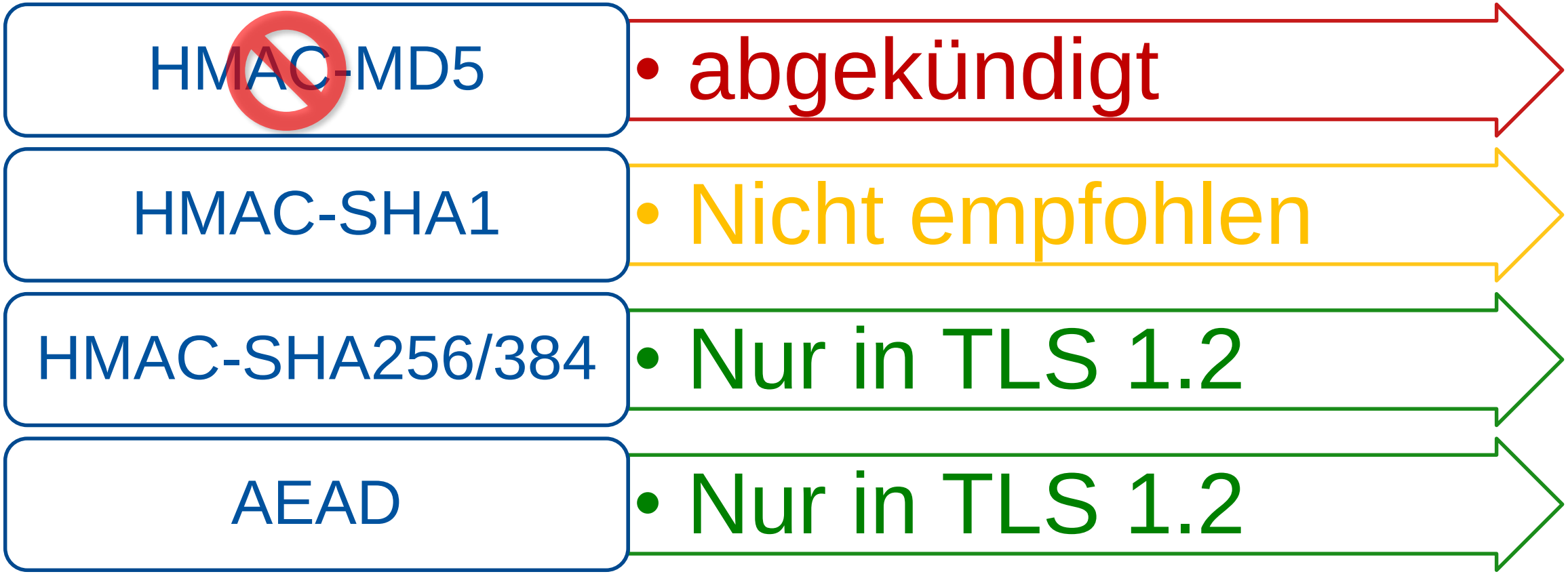
Sichere Block Cipher
mit Authenticated Encryption

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_3DES_EDE_CBC_SHA

Unsichere Block Cipher

Message Authentification



Was sagt das BSI?

	Schlüsseleinigung und -authentisierung		*Verschlüsselung*	*Betriebs-modus*	*Hash*	*Verwendung bis*
TLS_	ECDHE_ECDSA_	WITH_	AES_128_	CBC_ GCM_	SHA256	2024+
			AES_256_	CBC_ GCM_	SHA384	2024+
	ECDHE_RSA_	WITH_	AES_128_	CBC_ GCM_	SHA256	2024+
			AES_256_	CBC_ GCM_	SHA384	2024+
	DHE_DSS_[1]	WITH_	AES_128_	CBC_ GCM_	SHA256	2024+
			AES_256_	CBC_	SHA256	2024+
				GCM_	SHA384	2024+
	DHE_RSA_[1]	WITH_	AES_128_	CBC_ GCM_	SHA256	2024+
			AES_256_	CBC_	SHA256	2024+
				GCM_	SHA384	2024+

Nur TLS 1.2 ist empfohlen!

Quelle: BSI TR-02102-2

Mögliche Angriffsszenarien

- Padding attack
- Renegotiation attack
- Downgrade attacks
- Cross-protocol attacks
- BEAST attack
- CRIME and BREACH attacks
- Timing attacks on padding
- POODLE attack
- RC4 attacks
- Truncation attack
- Unholy PAC attack
- Sweet32 attack
- Implementation errors

- FREAK (MitM) und Logjam
- Server wird gezwungen eine schwache Cipher Suite zu verwenden
- dadurch Session Key escrow möglich.

- Schwachstelle in CBC : Mechanismus wie eFail
- RC4 als temporäre Lösung

- Entschlüsselung von Verbindungen mit relativ wenig Aufwand
- SSL 3.0
- TLS unter bestimmten Voraussetzungen ebenfalls

- Heartbleed bug : OPENSSL
- BERserk attack : NSS Libary
- Cloudbleed bug : Memory Leak NGINX

Fazit:

Lieber eine schlechte Verschlüsselung als keine, oder?

Ja, ABER:

Das Risiko muss kalkulierbar sein!

Noch unbekannte Implementierungsfehler sind reduzierbar durch gezieltes Ausstellten von Schlüsselmaterial welches einen potentiellen Downgrade im Keim erstickt.