

Das Integrationsverfahren in der Praxis: Zulassung der genugate-Firewall

Dr. Dirk Husfeld, genua GmbH
<dirk_husfeld@genua.de>

Kirchheim, 16. Januar 2020

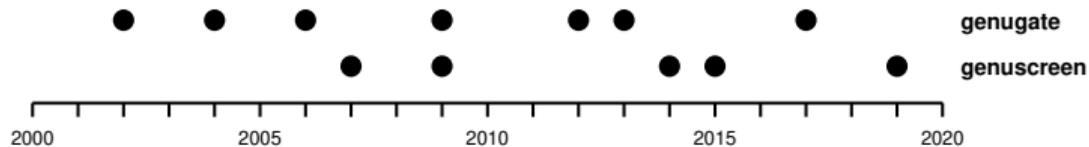


ZZ-Aktivitäten bei genua



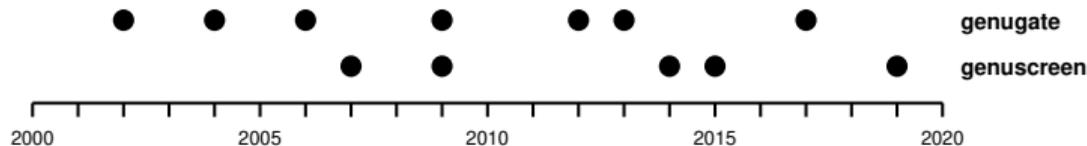
ZZ-Aktivitäten bei genua

- Zertifizierungen seit 2002, erst ITSEC, dann CC
Produkte genugate und genuscreen

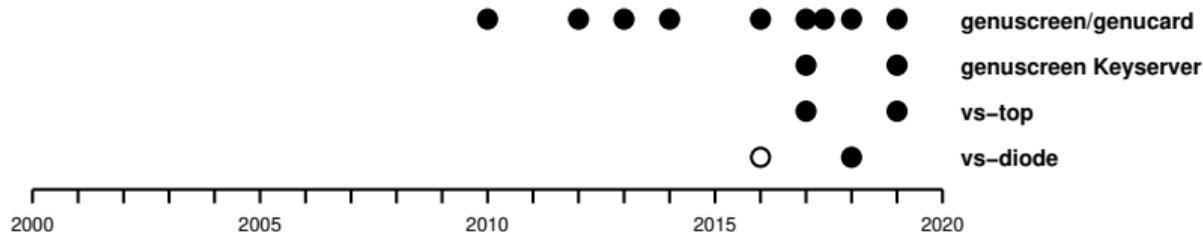


ZZ-Aktivitäten bei genua

- Zertifizierungen seit 2002, erst ITSEC, dann CC
Produkte genugate und genuscreen



- Zulassungen nach VSA seit 2010
Produkte genuscreen/genucard, keyserver, vs-top, vs-diode



Warum war die genugate-Firewall bislang nicht zugelassen?



Warum war die genugate-Firewall bislang nicht zugelassen?

- „Alte“ VSA (bis Mitte 2018) sah VS-NfD-Zulassungen nur für Kryptogeräte vor.



Warum war die genugate-Firewall bislang nicht zugelassen?

- „Alte“ VSA (bis Mitte 2018) sah VS-NfD-Zulassungen nur für Kryptogeräte vor.
- genugate ist „nur“ Firewall-System, enthält keine VPN-Funktionalität.

⇒ genugate konnte nach alter VSA nicht zugelassen werden.



Warum war die genugate-Firewall bislang nicht zugelassen?

- „Alte“ VSA (bis Mitte 2018) sah VS-NfD-Zulassungen nur für Kryptogeräte vor.
- genugate ist „nur“ Firewall-System, enthält keine VPN-Funktionalität.

⇒ genugate konnte nach alter VSA nicht zugelassen werden.

- Die VSA 2018 erweitert die zulassungsrelevanten IT-Sicherheitsfunktionen deutlich, u.a. um Informationsflusskontrolle und Netzwerktrennung



Warum war die genugate-Firewall bislang nicht zugelassen?

- „Alte“ VSA (bis Mitte 2018) sah VS-NfD-Zulassungen nur für Kryptogeräte vor.
- genugate ist „nur“ Firewall-System, enthält keine VPN-Funktionalität.

⇒ genugate konnte nach alter VSA nicht zugelassen werden.

- Die VSA 2018 erweitert die zulassungsrelevanten IT-Sicherheitsfunktionen deutlich, u.a. um Informationsflusskontrolle und Netzwerktrennung
- VSA-Zulassung von Firewalls nun möglich und **notwendig**

Erste Abstimmungen zur genugate-Zulassung

- Vorstellung des Integrationsverfahrens durch das BSI im Juli 2019



Erste Abstimmungen zur genugate-Zulassung

- Vorstellung des Integrationsverfahrens durch das BSI im Juli 2019
- Eindruck bei genua:
 - Grundidee des Verfahrens erscheint plausibel
 - Bedarf an Nachweisdokumenten ist nachvollziehbar
 - zentrale Bedeutung der neuen Assurance Class ADT_*

Erste Abstimmungen zur genugate-Zulassung

- Vorstellung des Integrationsverfahrens durch das BSI im Juli 2019
- Eindruck bei genua:
 - Grundidee des Verfahrens erscheint plausibel
 - Bedarf an Nachweisdokumenten ist nachvollziehbar
 - zentrale Bedeutung der neuen Assurance Class ADT_*
- genugate erscheint bestens geeignet:
 - CC-Zertifikat nach EAL4+ liegt vor.
 - Augmentation schließt u.a. Hochsicherheit nach AVA_VAN.5 ein.
 - weitere Verfahrenserleichterung durch genua-Status als Qualifizierter Hersteller (z.B. Life-Cycle-Nachweise)

Konkretes Vorgehen

- Projektstart September 2019
- basierend auf
 - CC-Zertifikat BSI-DSZ-CC-1039-2017 für genugate 9.0
 - VS-Anforderungsprofil (VSAP) Firewall 1.0 vom 20.05.2019
 - Anforderungskatalog "Nachweise für eine Delta-Evaluierung für eine Zulassung bis VS-NfD", Version 0.2 und folgende
- Ziel: Zulassung für VS-NfD im aktuellen Patch-Stand



Erfahrungen in der Praxis

- Conformance Claim „Produkttyp“ erfolgte in Absprache mit dem BSI (BSI-Produktkatalog lag noch nicht vor.)



Erfahrungen in der Praxis

- Conformance Claim „Produkttyp“ erfolgte in Absprache mit dem BSI (BSI-Produktkatalog lag noch nicht vor.)
- Rationale *Security Problem Definition* ok (zunächst informell)

Erfahrungen in der Praxis

- Conformance Claim „Produkttyp“ erfolgte in Absprache mit dem BSI (BSI-Produktkatalog lag noch nicht vor.)
- Rationale *Security Problem Definition* ok (zunächst informell)
- Rationale *Security Objectives* ok (zunächst informell)

Erfahrungen in der Praxis

- Conformance Claim „Produkttyp“ erfolgte in Absprache mit dem BSI (BSI-Produktkatalog lag noch nicht vor.)
- Rationale *Security Problem Definition* ok (zunächst informell)
- Rationale *Security Objectives* ok (zunächst informell)
- Rationale *Security Functional Requirements* erforderte Diskussion bzgl. mehrerer Punkte, z.B.:

Erfahrungen in der Praxis

- Conformance Claim „Produkttyp“ erfolgte in Absprache mit dem BSI (BSI-Produktkatalog lag noch nicht vor.)
- Rationale *Security Problem Definition* ok (zunächst informell)
- Rationale *Security Objectives* ok (zunächst informell)
- Rationale *Security Functional Requirements* erforderte Diskussion bzgl. mehrerer Punkte, z.B.:
 - Umgang mit Updates/Patches

Erfahrungen in der Praxis

- Conformance Claim „Produkttyp“ erfolgte in Absprache mit dem BSI (BSI-Produktkatalog lag noch nicht vor.)
- Rationale *Security Problem Definition* ok (zunächst informell)
- Rationale *Security Objectives* ok (zunächst informell)
- Rationale *Security Functional Requirements* erforderte Diskussion bzgl. mehrerer Punkte, z.B.:
 - Umgang mit Updates/Patches
 - Kryptofunktionen

Konsequenzen der Erfahrungen

- Erfahrungsaustausch mit BSI Mitte September, Update des Anforderungskatalogs



Konsequenzen der Erfahrungen

- Erfahrungsaustausch mit BSI Mitte September, Update des Anforderungskatalogs
- Zuordnung (*mapping*) für *Security Problem Definition* und *Security Objectives* nachholen



Konsequenzen der Erfahrungen

- Erfahrungsaustausch mit BSI Mitte September, Update des Anforderungskatalogs
- Zuordnung (*mapping*) für *Security Problem Definition* und *Security Objectives* nachholen
- Mehrstufigkeit der Schutzfunktionen im Produkt ausnutzen, dazu entsprechende Auflagen in den Einsatz- und Betriebsbedingungen



Weiteres Vorgehen

- Zulassung einer aktuellen genugate-Version
 -



Weiteres Vorgehen

- Zulassung einer aktuellen genugate-Version
 - per Integrationsverfahren basierend auf genugate 10.0?



Weiteres Vorgehen

- Zulassung einer aktuellen genugate-Version
 - ~~per Integrationsverfahren basierend auf genugate 10.0?~~
 - per Qualifiziertem Verfahren für genugate 9.6?

Weiteres Vorgehen

- Zulassung einer aktuellen genugate-Version
 - ~~per Integrationsverfahren basierend auf genugate 10.0?~~
 - per Qualifiziertem Verfahren für genugate 9.6 !! ← Zeitvorteil

Weiteres Vorgehen

- Zulassung einer aktuellen genugate-Version
 - ~~per Integrationsverfahren basierend auf genugate 10.0?~~
 - per Qualifiziertem Verfahren für genugate 9.6 !! ← Zeitvorteil
 - Ziel: Zulassung von genugate 9.6 im Quartal II/2020

Weiteres Vorgehen

- Zulassung einer aktuellen genugate-Version
 - ~~per Integrationsverfahren basierend auf genugate 10.0?~~
 - per Qualifiziertem Verfahren für genugate 9.6 !! ← Zeitvorteil
 - Ziel: Zulassung von genugate 9.6 im Quartal II/2020
- Allgemeine Abwägung (basierend auf genua-Verhältnissen)
 - Integrationsverfahren ist deutlich schneller als Zulassung von Grund auf, *wenn Zertifizierung bereits vorliegt.*

Weiteres Vorgehen

- Zulassung einer aktuellen genugate-Version
 - ~~per Integrationsverfahren basierend auf genugate 10.0?~~
 - per Qualifiziertem Verfahren für genugate 9.6 !! ← Zeitvorteil
 - Ziel: Zulassung von genugate 9.6 im Quartal II/2020
- Allgemeine Abwägung (basierend auf genua-Verhältnissen)
 - Integrationsverfahren ist deutlich schneller als Zulassung von Grund auf, *wenn Zertifizierung bereits vorliegt.*
 - Aktualisierung einer Zulassung durch Update bestehender Nachweisdokumente verursacht etwa vergleichbaren Aufwand.

Weiteres Vorgehen

- Zulassung einer aktuellen genugate-Version
 - ~~per Integrationsverfahren basierend auf genugate 10.0?~~
 - per Qualifiziertem Verfahren für genugate 9.6 !! ← Zeitvorteil
 - Ziel: Zulassung von genugate 9.6 im Quartal II/2020
- Allgemeine Abwägung (basierend auf genua-Verhältnissen)
 - Integrationsverfahren ist deutlich schneller als Zulassung von Grund auf, *wenn Zertifizierung bereits vorliegt.*
 - Aktualisierung einer Zulassung durch Update bestehender Nachweisdokumente verursacht etwa vergleichbaren Aufwand.
 - Warten auf den Abschluss einer Zertifizierung und folgendes Integrationsverfahren ist i.d.R. ineffektiv.

Vielen Dank!
Weitere Fragen?

