SECURITY PUPPY

Certificate Policy

Hartanto Ario Widjaya

hartanto@securitypuppy.com

securitypuppy.com

Version 1.2

10 February 2021

Version History

Version	Date	Details
1.0	22 December 2018	First Release
1.1	01 October 2019	Add GitHub Signing Key
1.2	10 February 2021	Change DocuSign Certificate

Primary PGP Key Details

Name	Hartanto Ario Widjaya
Email Address	hartanto@securitypuppy.com
Creation Date	June 1st 2018
Type	*Elliptical Curve Cryptography*
Primary Key	Certification
Fingerprint	A198 07CE 3472 EADE 98BF 030E EEB1 D3AF 8CF1 C236
Curve	ed25519
Expiry	Never
Subkey	Signing
Fingerprint	5C58 4254 BCEC D361 AA46 8B18 91A2 F9BD 7A17 E1CC
Curve	ed25519
Expiry	Never
Subkey	Authentication
Fingerprint	24B4 DD29 81B1 D56A A16F 1D72 B1CD 2D78 4DAD B915
Curve	ed25519
Expiry	Never
Subkey	Encryption
Fingerprint	9F5A 4720 3351 E96B E1C6 A168 8876 AD10 9745 7959
Curve	cv25519
Expiry	Never

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEWxCx3xYJKwYBBAHaRw8BAQdAgy7L1K1uSQA4chrh0lOcGXGEuwnPJ3WLMlzE
OT29Xj60MkhhcnRhbnRvIEFyaW8gV2lkamF5YSA8aGFydGFudG9Ac2VjdXJpdHlw
dXBweS5jb20+iJAEExYIADgWIQShmAfONHLq3pi/Aw7usdOvjPHCNgUCWxCx3wIb
AQULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRDusdOvjPHCNkiGAP42kNvmr1Tc
0TqS11w08XWUV2yZ33qxAoaEtNriCdCBEAD5Af7V5N9sAUiH3kuRHMbuxV0Tfwji
xBuYgYwoqvACZwe4MwRbELIOFgkrBgEEAdpHDwEBB0BCD1QTlizWrL2iOsKVftf/
VIKRm9Ll4l3JdKie0pPGPIjvBBgWCAAgFiEEoZgHzjRy6t6YvwMO7rHTr4zxwjYF
AlsQsg4CGwIAgQkQ7rHTr4zxwjZ2IAQZFggAHRYhBFxYQlS87NNhqkaLGJGi+b16
F+HMBQJbELIOAAoJEJGi+b16F+HMV+IA/AzZUcmn3S+m3KCZtr8/wS2VSOuYA5D/
0M7T1saNBpJ7AP9lXTtbXDTnmcIP8Vcn/PYuQ0rXZxPRhffIWMi2cpw7CAmaAP9E
0apJpaVB4GGrsXtvHafUkE5uLGAlzyxd5USpnHN+7QEAxBBFP/0n9f5feUUDEXx8
0fmYMpuz0ATTqgehyOu5XAq4MwRbELIrFgkrBgEEAdpHDwEBB0Ax09Kxz7qoEz6f
kwGP876pBv3F94oQhnHnfg6ptZc1rIh4BBgWCAAgFiEEoZgHzjRy6t6YvwMO7rHT
r4zxwjYFAlsQsisCGyAACgkQ7rHTr4zxwjbH3wD8DA10YDL9yJAyUbDm2hvOKsgv
735LJd97BMCMBVU1++cBAKE/xUbxwK6bEd/6KBJHvQyKmFgS5Xi3pjMbqwvU40kD
uDgEWxCyTRIKKwYBBAGXVQEFAQEHQMxL280j4xSrVVnr8OCUjOAbMKxqPcRNktWQ
BhfEdJJlAwEIB4h4BBgWCAAgFiEEoZgHzjRy6t6YvwMO7rHTr4zxwjYFAlsQsk0C
GwwACgkQ7rHTr4zxwjaDgAEApgY7XOIG+UeGCCbvxu2gCTgcyJZk87A67J5yLtwe
jsMA/2r24L2L1dBD0ZV91VuMj+9MoMuftsVgXYxfQFnlRlgC
=SIXk
-----END PGP PUBLIC KEY BLOCK-----
```

SECURITY PUPPY

GitHub Signing PGP Key Details

Name	Hartanto Ario Widjaya
Email Address	tanto259@users.noreply.github.com
Creation Date	October 1st 2019
Type	*Elliptical Curve Cryptography*
Primary Key	**Certification and Signing**
Fingerprint	16D7 7EBF 86E5 DA6A 1FE2 F0B2 1F16 639C 2A37 BEF8
Curve	ed25519
Expiry	Never

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEXZLgJRYJKwYBBAHaRw8BAQdA8bDn6KAwgBARDqJ7kFzsRJl/b0iYmEoukZ/F
PaRSPHS0TkhhcnRhbnRvIEFyaW8gV2lkamF5YSAoR2l0SHViIFNpZ25pbmcgS2V5
KSA8dGFudG8yNTlAdXNlcnMubm9yZXBseS5naXRodWIuY29tPoiQBBMWCAA4FiEE
Ftd+v4bl2mof4vCyHxZjnCo3vvgFAl2S4CUCGwMFCwkIBwIGFQoJCAsCBBYCAwEC
HgECF4AACgkQHxZjnCo3vvgK5QD8D2TAYGSwY4LDYWL/xy05EtBNiUzeDTl71S5Z
jDPsc3wBAIPnMHLsQZ1wi6Y4aY7CSf2M5hMlJ2O0wotdflHtlSkJiHUEEBYIAB0W
IQShmAfONHLq3pi/Aw7usdOvjPHCNgUCXZMU0QAKCRDusdOvjPHCNopeAPsGWEyQ
HN4CZuVPvZyGBvte2V0psc1UsUO8QrDclwT0cQEA1NcaDN+wVumVJ8llkeBFcj9U
Onqixkjs7vg7yYZKjAw=
=Q18X
-----END PGP PUBLIC KEY BLOCK-----
```

Electronic Signature Details

This electronic signature is issued by DocuSign

Signature:

DocuSigned by:

Hartanto Ario Widjaya

FB1325E4E1D7407...

Documents are signed using the DocuSign's X.509 Certificate, the certificate can be found at *https://www.docusign.com/trust/compliance/public-certificates.*

The certificate has the following details:

Serial Number	48A939FF10324D75DA565BCEE491D5F4

Subject	E = enterprisesupport@docusign.com
	CN = DocuSign, Inc.
	OU = Technical Operations
	O = DocuSign, Inc.
	L = San Francisco
	S = California
	C = US

Issuer	CN = Entrust Class 3 Client CA - SHA256
	OU = (c) 2015 Entrust, Inc. - for authorized use only
	OU = See www.entrust.net/legal-terms
	O = Entrust, Inc.
	C = US

Valid From	Saturday, August 8, 2020 7:47:51 AM
Valid To	Wednesday, December 21, 2022 7:47:50 AM
Subject Key Identifier	BA2F47FFC325AD1A2680B8419BB9FCFA90331D06

DocuSign is an electronic signature provider based in the United States.

DocuSign have high security certification standards with ISO27001:2013, SOC1 and SOC2 certification. More details at *https://www.docusign.com/trust.*

1.0 Preamble

This policy governs the way I, acting as SecurityPuppy.com, signs documents and keys using either the OpenPGP protocol (formalised by RFC4880) or the X.509 PKI certificate (formalised by RFC5280) through DocuSign.

This policy applies to the PGP keys and DocuSign electronic signature listed on the previous pages. For formality, the current Primary PGP key fingerprint is A19807CE3472EADE98BF030EEEB1D3AF8CF1C236, the current GitHub Signing PGP key fingerprint is 16D77EBF86E5DA6A1FE2F0B21F16639C2A37BEF8 along with the first 16 bit of my DocuSign customer ID FB1325E4E1D7407.

The PGP keys does not have any expiry date, but I reserve the right to revoke or change the keys for any reason without prior notice. The X.509 certificate has a one-year expiry and may be renewed without prior notice. Should there be a change in either the expiry or the keys/certificate themselves, this policy will be updated to reflect the change.

1.1 PGP Key Signing

For this policy, the signing convention trust level listed on RFC4880 will be adopted here as follows:

- 0x10: Generic certification of a User ID or Public-Key packet. I do not make any assertion to how well I have checked that the owner of the key is in fact the person described by the User ID.
- 0x11: Persona certification of a User ID or Public-Key packet. I have not done any verification of the claim that the owner of this key is the User ID specified.
- 0x12: Casual certification of a User ID or Public-Key packet. I have done some casual verification of the claim of identity.
- 0x13: Positive certification of a User ID or Public-Key packet. I have done substantial verification of the claim of identity.

The usage of the trust level is as follow:

0x10	Public-Key packet with a corporation as the User ID or Signing-only Key packet on behalf of an individual as long as the individual has at least one Public-Key packet signed on either 0x12 or 0x13.
0x11	I will not sign any Public-Key packet at this level.
0x12	Public-Key packet of individual I know.
0x13	Public-Key packet of individual I closely know.

The following requirements are necessary for signing:

0x10	*Corporate Public-Key Packet:* The key is listed on the corporation website, with at least one email listed on the User ID under the same domain as the website where the key is found. *Personal Signing-only Key Packet:* The person on the User ID contacted me with a signed message from the higher trust level key requesting the signage of this Signing-only Key packet.
0x12	I have met the person on the User ID. Verification of a government-issued identification is required. I will send an encrypted message with a string of word to the email(s) listed on the User ID as a verification method.
0x13	I have known the person on the User ID for at least 1 (one) year. Verification of two forms of ID, one of which must be a government-issued identification, is required. I will send an encrypted message with a string of word to the email(s) listed on the User ID as a verification method.

The person listed on the User ID should send a message requesting the signing of the Public-Key packet from the email address listed on the User ID. The message should contain the Public-Key packet. Please note that the signing will only take place in person. The signing will be done with my Primary PGP Key as indicated above.

I reserve the right to reject the given signing request for any reason without prior notice.

As a note, here is a comparison between the trust level listed on RFC4880 and GnuPG.

0x10	I do not know or won’t say
0x11	I do NOT trust
0x12	I trust marginally
0x13	I trust fully

At any time, the person listed on the User ID may request a revocation of the given signature, to do that the person must send me a signed message requesting revocation. Should the person lost access to the PGP key, I will not revoke the signature prior to the expiry of the key. After the expiry of the key plus an additional 14 days, I may choose to revoke the certificate if I consider such revocation necessary.

In the event of the creation of a new Public-Key packet, the person listed on the User ID may request the signing on the new key. To do that, the person must send me a message requesting such action which is signed by the previous key. In the message, the person must include the new Public-Key packet. Should the new User ID contain at least one different email address, I will send an encrypted message with a string of word to the new email(s) listed on the User ID as a verification method.

Any message requesting either revocation or (re)signing must be sent through the email address listed on the User ID of the Public-Key packet to *hartanto@securitypuppy.com*.

I reserve the right to reject any revocation or resigning request for any reason. User ID with only pseudonym name will not be signed. Additionally, I reserve the right to revoke the given signature for any reason without prior notice.

1.2 GitHub Commits and Tags Signing

All GitHub commits and tags committed by me will be signed using the GitHub Signing PGP key as indicated above. For formality, my username at GitHub is tanto259.

1.3 Document Signing

For signing a formal Portable Document Format or PDF, the use of electronic signature, as listed previously, is preferred. Please note that I do not hold the private key myself.

The digital signature is issued through DocuSign and may be considered legally binding.

All other documents, including emails and non-formal PDF, will be signed using the Primary PGP Key. The use of detached or standalone signature (0x02) is preferred.

I reserve the right to reject document signing for any reason without prior notice.

1.4 Verification

To verify that I have access to both the Primary PGP key and the DocuSign electronic signature listed previously, this document will be signed by the DocuSign signature and a detached PGP signature will be included. Additionally, to verify my access to the GitHub PGP signing key, I will sign the key using my Primary PGP key.

Signed on the 10th of February 2021,

DocuSigned by:

Hartanto Ario Widjaya

FB1325E4E1D7407...

Hartanto Ario Widjaya

-end of document-

DocuSign SECURED

Certificate Of Completion

Envelope Id: 7E1019A15FCE47ECAC78F54DB0B4E5B0		Status: Completed
Subject: Please DocuSign: SecurityPuppy_CP1.2.pdf		
Source Envelope:		
Document Pages: 9	Signatures: 1	Envelope Originator:
Certificate Pages: 1	Initials: 0	Hartanto Ario Widjaya
AutoNav: Enabled		hartanto@securitypuppy.com
EnvelopeId Stamping: Enabled		IP Address: 202.161.35.27
Time Zone: (UTC-08:00) Pacific Time (US & Canada)		

Record Tracking

Status: Original 2/9/2021 9:52:03 PM	Holder: Hartanto Ario Widjaya hartanto@securitypuppy.com	Location: DocuSign

Signer Events	Signature	Timestamp
Hartanto Ario Widjaya hartanto@securitypuppy.com SecurityPuppy.com Security Level: Email, Account Authentication (None)	DocuSigned by: Hartanto Ario Widjaya FB1325E4E1D7407... Signature Adoption: Pre-selected Style Using IP Address: 202.161.35.27	Sent: 2/9/2021 9:52:15 PM Viewed: 2/9/2021 9:52:21 PM Signed: 2/9/2021 9:52:50 PM Freeform Signing

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	2/9/2021 9:52:15 PM
Certified Delivered	Security Checked	2/9/2021 9:52:21 PM
Signing Complete	Security Checked	2/9/2021 9:52:50 PM
Completed	Security Checked	2/9/2021 9:52:50 PM

Payment Events	Status	Timestamps