



life.augmented



presented by
EBVElektronik
| An Avnet Company |

STM32Trust

More Trust with STM32



A whole security ecosystem around STM32

STM32Trust offers a robust multi-level strategy to enhance security in new product designs utilizing our STM32 Microcontrollers & microprocessor augmented with STSAFE secure elements.

STM32Trust is the security framework combining our knowledge, ecosystem and security services.

The solution offers a complete toolset for code and execution protection, ensures IP protection, data secured, and validated credentials are used, and helps to get firmware authenticity and secure firmware update.

THE SECURITY FUNCTIONS

STM32Trust offer results for accurate analysis of customer cases, ending up in the coverage of the base 12 security functions required for their needs

- Secure Boot
- Secure Install/Update
- Secure Storage
- Isolation
- Abnormal situations handling
- Crypto Engine
- Audit/Log
- Identification / Authentication / Attestation
- Silicon Device Lifecycle
- Software IP Protection
- Secure Manufacturing
- Application Lifecycle

All statements are without any engagement. Subject to modifications and amendments. F-245-E-01-2021-V1

STM32Trust | MORE TRUST WITH STM32

1- Secure boot

Ability to ensure the authenticity and integrity of an application that is inside a device

2- Secure Install/Update

Installation or update of firmware with initial checks of integrity and authenticity before programming and executing

3- Secure Storage

Ability to securely store secrets like data or keys

4- Isolation

Isolation between trusted and non-trusted parts of an application

5- Abnormal situations handling

Ability to detect abnormal situations (both hardware and software) and to take adapted decisions like secrets removals

6- Crypto Engine

Ability to process cryptographic algorithms, as recommended by a security assurance level

7- Audit/Log

Keep trace of security events in an unchangeable way

8- Identification / Authentication / Attestation

Unique identification of a device and/or software, and ability to detect its authenticity, inside the device or externally

9- Silicon Device Lifecycle

Control states to securely protect silicon device assets through a constrained path

10- Software IP Protection

Ability to protect a section or the whole software against external or internal reading. Can be multi-tenant

11- Secure Manufacturing

Initial device provisioning in unsecured environment with overproduction control. Potential secured personalization

12- Application Lifecycle

Define unchangeable incremental states to securely protect application states and assets

Those 12 Security Functions are completely or partially covered by ST offers, with combinations of hardware, software tools and services

Security function	STM32F4/F7/L1/WB/G0/G4/H7/L0/L4		STM32MP1		STM32L5 WITH TRUSTZONE		+ STSAFE-A/TPM
	Silicon	Firmware	Silicon	Firmware	Silicon	Firmware	Silicon
Secure boot	✓		✓	TF-A	✓		✓
Secure Install/Update	✓	SBSFU	✓	OPTEE	✓	TFM_SBSFU	✓
Secure Storage	(L0/L4/H7/G0/G4)	(WB) SBSFU KMS	✓	OPTEE	✓	TFM_SPE	✓
Isolation	✓		✓	OPTEE	✓	TFM	✓
Abnormal situations handling	✓		✓		✓		
Crypto Engine	✓	Crypto libraries	✓	OPTEE	✓	Crypto libraries TFM	✓
Audit/Log					✓	TFM	
Identification / Authentication / Attestation	✓		✓		✓	TFM Attestation	✓
Silicon Device Lifecycle	✓		✓		✓		
Software IP Protection	✓		✓	OPTEE	✓	TFM	
Secure Manufacturing	SFI (H7/L4) with STM32HSM		SSP with STM32HSM		SFI with STM32HSM		✓
Application Lifecycle	✓		✓		✓		✓

*All those solutions are defined at www.st.com/stm32trust

■ Reference firmware proposed by ST
■ Firmware to be developed by user

CERTIFICATIONS

ST is fully committed at certifying its solutions by independent recognized authority.

To discover this complete offer, please visit www.st.com/stm32trust

Available now

CERTIFICATIONS



ARM PSA

- Level 1
STM32L4
STM32L5
- Level 2
STM32L5 (TFM)
- API Compliant
STM32L5 (TFM)



COMMON CRITERIA

- CC EAL5+
STSAFE-A110
STSAFE-TPM



SESIIP

- Level 1
STM32L4 (SBSFU)
- Level 3
STM32L4 (SBSFU)



PCI

- Point of Sale application
STM32L4

EBV European Headquarters

EBV Elektronik GmbH & Co. KG | DE-85586 Poing | Im Technologiepark 2-8 | Phone: +49 8121 774 0

EBV Regional Offices | Status January 2021

AUSTRIA

1120 Wien
Grünbergstraße 15/1, 4. Stock
Phone: +43 1 89152 0
Fax: +43 1 89152 30

BELGIUM

1831 Diegem
De Kleetlaan 3
Phone: +32 2 716001 0
Fax: +32 2 72081 52

BULGARIA

1505 Sofia
48 Sitnyakovo Blvd., Serdika
offices, 10th floor, Unit 1006
Phone: +359 2 9264 337
Fax: +359 2 9264 133

CZECH REPUBLIC

18600 Prague
Amazon Court, Karolinska 661/4
Phone: +420 2 34091 011
Fax: +420 2 34091 010

DENMARK

8230 Åbyhøj
Ved Lunden 10-12, 1. sal
Phone: +45 8 6250 466
Fax: +45 8 6250 660

ESTONIA

80042 Pärnu
Suur-Jõe 63
Phone: +372 5 8864 446

FINLAND

02240 Espoo
Pihatörmä 1a
Phone: +358 9 2705279 0
Fax: +358 9 27095498

FRANCE

90100 Oulu
Nahkatehtaankatu 2
Phone: +358 8 4152627 0
Fax: +358 8 4152627 5

FRANCE

91300 Massy Cedex (Paris)
Le Copernic bât B
12 rue Jean Bart
Phone: +33 1 644729 29

35510 Cesson Sévigné (Rennes)
35, av. des Peupliers
Phone: +33 2 998300 51
Fax: +33 2 998300 60

67400 Illkirch Graffenstaden
35 Rue Gruninger
Phone: +33 3 904005 92
Fax: +33 3 886511 25

31500 Toulouse
8 chemin de la terrasse
Parc de la plaine
Phone: +33 5 610084 61
Fax: +33 5 610084 74

69693 Venissieux (Lyon)
Parc Club du Moulin à Vent
33, Av. du Dr. Georges Lévy
Phone: +33 4 727802 78
Fax: +33 4 780080 81

GERMANY

85609 Aschheim-Dornach
Einsteinring 1
Phone: +49 89 388 882 0
Fax: +49 89 388 882 020

10553 Berlin
Kaiserin-Augusta-Allee 14
Phone: +49 30 747005 0
Fax: +49 30 747005 55

30938 Burgwedel
Burgdorfer Straße 2
Phone: +49 5139 8087 0
Fax: +49 5139 8087 70

59439 Holzwickede
Wilhelmstraße 1
Phone: +49 2301 94390 0
Fax: +49 2301 94390 30

41564 Kaarst
An der Gümpgesbrücke 7
Phone: +49 2131 9677 0
Fax: +49 2131 9677 30

71229 Leonberg
Neue Ramtelstraße 4
Phone: +49 7152 3009 0
Fax: +49 7152 759 58

90471 Nürnberg
Lina-Ammon-Straße 19B
Phone: +49 911 817669 0
Fax: +49 911 817669 20

04435 Schkeuditz
Frankfurter Straße 2
Phone: +49 34204 4511 0
Fax: +49 34204 4511 99

78048 VS-Villingen
Marie-Curie-Straße 14
Phone: +49 7721 99857 0
Fax: +49 7721 99857 70

65205 Wiesbaden
Borsigstraße 36
Phone: +49 6122 8088 0
Fax: +49 6122 8088 99

HUNGARY

1117 Budapest
Budafoki út 91-93, West Irodaház
Phone: +36 1 43672 29
Fax: +36 1 43672 20

ISRAEL

4581500 Bnei Dror
Tirosh 1
Phone: +972 9 77802 60
Fax: +972 3 76011 15

ITALY

20095 Cusano Milanino (MI)
Via Alessandro Manzoni, 44
Phone: +39 02 660962 90
Fax: +39 02 660170 20

50019 Sesto Fiorentino (FI)
Via Lucchese, 84/B
Phone: +39 05 543693 07
Fax: +39 05 542652 40

41126 Modena (MO)
Via Scaglia Est, 33
Phone: +39 059 292 4211
Fax: +39 059 292 9486

00139 Roma (RM)
Via de Settebagni, 390
Phone: +39 06 4063 665/789
Fax: +39 06 4063 777

35030 Sarmeola di Rubano (PD)
Piazza Adelaide Lonigo, 8/11
Phone: +39 049 89747 01
Fax: +39 049 89747 26

10144 Torino (TO)
Via Treviso, 16
Phone: +39 011 26256 90
Fax: +39 011 26256 91

IRELAND

Fitzwilliam Hall
Fitzwilliam Place
Dublin 2
D02 T292
Phone: +353 1 4097 802
Fax: +353 1 4568 544

NETHERLANDS

Zonnebaan 9
3542 EA Utrecht
Phone: +31 346 5830 10
Fax: +31 346 5830 25

NORWAY

3440 Røyken
Kleiverveien 35
Phone: +47 22 67 17 80
Fax: +47 22 67 17 89

POLAND

80-838 Gdansk
Targ Rybny 11/12
Phone: +48 58 30781 00

P02-676 Warszawa
Postepu 14
Phone: +48 22 209 88 05

50-062 Wrocław
Pl. Solny 16
Phone: +48 71 34229 44
Fax: +48 71 34229 10

PORTUGAL

4400-676 Vila Nova de Gaia Unipessoal
LDA / Edifício Tower Plaza
Rotunda Eng. Edgar Cardoso, 23 - 14ºG
Phone: +351 22 092026 0
Fax: +351 22 092026 1

ROMANIA

020334 Bucharest
4C Gara Herastrau Street
Building B, 2nd Floor - 2nd District
Phone: +40 21 52816 12
Fax: +40 21 52816 01

RUSSIA

620028 Ekaterinburg
Tatischeva Street 49A
Phone: +7 343 31140 4
Fax: +7 343 31140 46

127486 Moscow
Korovinskoye Shosse 10,
Build 2, Off. 28
Phone: +7 495 730317 0
Fax: +7 495 730317 1

197374 St. Petersburg
Atlantic City, Savushkina str 126,
lit B, premises 59-H, office 17-2
Phone: +7 812 635706 3
Fax: +7 812 635706 4

SERBIA

11070 Novi Beograd
Milentija Popovica 5B
Phone: +381 11 40499 01
Fax: +381 11 40499 00

SLOVAKIA

82109 Bratislava
Turcianska 2 Green Point Offices
Phone: +421 2 3211114 1
Fax: +421 2 3211114 0

SLOVENIA

1000 Ljubljana
Dunajska cesta 167
Phone: +386 1 5609 778
Fax: +386 1 5609 877

SOUTH AFRICA

7700 Rondebosch, Cape Town
Belmont Office Park, Belmont Road
1st Floor, Unit 0030
Phone: +27 21 402194 0
Fax: +27 21 4196256

3629 Westville
Forest Square, 11 Derby Place
Suite 4, Bauhinia Building
Phone: +27 31 27926 00
Fax: +27 31 27926 24

2128 Rivonia, Sandton
Johannesburg
33 Riley Road
Pinewood Office Park
Building 13, Ground Floor
Phone: +27 11 23619 00
Fax: +27 11 23619 13

SPAIN

08014 Barcelona
c/ Tarragona 149 - 157 Planta 19 1º
Phone: +34 93 47332 00
Fax: +34 93 47363 89

39005 Santander (Cantabria)
Racing nº 5 bajo
Phone: +34 94 22367 55
Phone: +34 94 23745 81

28760 Tres Cantos (Madrid)
c/ Ronda de Poniente 14 - 2ª planta
Phone: +34 91 80432 56
Fax: +34 91 80441 03

SWEDEN

16440 Kista
Isafjordsgatan 32B, Floor 6
Phone: +46 859 47023 0
Fax: +46 859 47023 1

SWITZERLAND

8953 Dietikon
Bernstrasse 394
Phone: +41 44 74561 61
Fax: +41 44 74561 00

TURKEY

06520 Ankara
Armada Is Merkezi
Eskisehir Yolu No: 6, Kat: 14
Ofis No: 1406, Sogutozu
Phone: +90 312 2956 361
Fax: +90 216 528831 1

34774 Ümraniye / Istanbul
Tatlısu Mahallesi Pakdil Sokak 7
Phone: +90 216 528831 0
Fax: +90 216 528831 1

35580 Izmir
Folkart Towers
Manas Blv. No 39 B Blok
Kat: 31 Ofis: 3121
Phone: +90 232 390 9196
Fax: +90 216 528831 1

UKRAINE

03040 Kiev
Vasilovskaya str. 14
off. 422-423
Phone: +380 44 496222 6
Fax: +380 44 496222 7

UNITED KINGDOM

Maidenhead (South)
Berkshire, SL6 7RJ
2, The Switchback
Gardner Road
Phone: +44 16 28778556
Fax: +44 16 28783811

Manchester (North)
M22 5WB
Manchester International Office Centre
Suite 3E (MIOC) Styal Road
Phone: +44 16 149934 34
Fax: +44 16 149934 74