			Microchip	STMicroelectronics	Infineon	NXP	
			ATECC608A	STSAFE-A100	Optiga Trust M	A71CH	A1006
local host interface			I²C or SWI (plus GPIO)	I²C	I²C	I²C	I²C or OWI
Public-Key crypto algorithms		ECC ECDSA	NIST P256	NIST or Brainpool 256/384 bit	NIST P521 & Brainpool 512	NIST P256	NIST B163
		RSA	-	-	1024/2048 bit	-	-
Hash algorithms		SHA-256	x	x	x	x	-
		SHA-384	-	x	-	-	-
		SHA-224	-	-	-	-	x
public key crypto toolbox	Authentication (sign/verify)	algorithms	ECC	ECC	ECC, RSA	ECC	ECC
	Secure-channel key agreement		ECDH	ECDH, ECDHE	ECDH, ECDHE	ECDH, ECDHE	ECDHE
	protocol support		TLS 1.2 & 1.3	TLS 1.2	TLS 1.2 & 1.3	TLS 1.2	
	Generation of new key pair		yes	yes	yes (ECC, RSA)	yes	no
	PKI or IoT Cloud support	Microsoft Azure	yes		yes	-	n/a
		AWS	yes		yes	yes	
		Google IoT Core	yes		-	yes	
		IBM Watson IoT	-		-	yes	
		Customer CA	yes	yes (ST needed)	yes (IFX needed)	yes	
		other					fixed unique key pair + certificate
pre-provisioned individual device identity			A: with 72-bit serial number only TLS: with generic certificates for IoT networks	serial number + unique ECC NIST-P-256 key pair incl. certificate	unique ECC key pair + certificate (IFX root CA)	yes + "root of trust"	n/a
User data memory (for keys, certificates)			yes	6kB	certificates, keys + 4.5kB	keys + 4kB	2 kbit certificates and 1kbit user (0,5 kB total)
Symmetric algorithms		AES-128	x	x	x	x	no
		AES-256	-	x	x	-	no
symmetric crypto toolbox	Authentication (sign/verify)		yes	yes	yes	HKDF	no
	Data encrypt/decrypt ("wapping")		yes	yes	yes		no
secure counters (usage monitoring)			yes, two	yes	yes, four	yes, two	no
security certificate (***)			-	EAL5+	EAL6+	CRI patent license	list of applied countermeasures
Electrical Characteristics	Power Supply	min (V)	2,0	1,6	1,62	2,5	1,62
		max (V)	5,5	5,5	5,5	3,6	3,6
	Operating Temperature	min (°C)	-40	-40	-25/-40	-25/-40	-25
		max (°C)	+85	+105	+85/+105	+85/+90	+85
	Power Consumption	$I_{CC-PROC}$	14mA (max.)	18mA (typ.)	20mA (typ.)	15,1mA (max.)	0,55 mA (max.)
		$I_{CC-STDBY}$	800µA (typ.)	245µA (typ.)	70µA (typ.)	45µA (typ.)	
		$I_{CC-HIBERNATE}$	2 µA (max.)	1,1µA (typ.)	<2,5µA (typ.)	10 µA (max.)	3,3 µA (max.)
Reliability	Data Retention		30 yrs (min. at +35°C)	30 yrs (at +25°C)		25 yrs (at +55°C)	25 yrs (at +55°C)
			10 yrs (min. at +55°C)				
	Write Endurance		400k (min. at +85°C)	500k (at +25°C)		500k	500k
Package			SO8N (4,9x6mm), UDFN8 (2x3mm)	SO8N (4x5mm), UFDFPN8(2x3mm)	PG-USON-10-2,4 (3x3mm)	HVSON-8 (4x4mm)	HXSON-6 (2x2mm)
Customer-specific Provisioning Service			yes (MOQ: 2 or 4 ku)	yes (MOQ: 5ku)	yes	yes (MOQ: 150ku)	
documentation of API, command set			public (after user registration)	under NDA	public (on github)	public (after user registration)	
Development Tools			CryptoAuth Trust Platform using a Microchip SAM D21 host MCU. Github section containing documentation, code examples.	X-NUCLEO-SAFEA1 expansion board (Arduino-compliant) to be used with any STM32 Nucleo development board. Including STSAFE API and sample demo code incl. secure boot and fw update	Trust M Shield2Go board for use with XMC4800 IoT eva board. Github section conbating Trust M Library, code examples for use cases, Trust M CA certificates.	A71CH board (Arduino-compliant) for use with 1) Kinetis (ARM Cortex) board with A71CH Host API, A71CH Config Tool, mbedTLS sw stack 2) MX6 based board Linux with A71CH Host API, A71CH Config Tool, Open SSL example	A1006 board (Arduino-compliant) incl A1006 host reference source code for use with LPCXpresso board (ARM mbed). Can also be used for provisioning user's certificate into A1006.
Online Support (**)			private support ticket, Community	private support ticket, forum	private support ticket, forum	private support ticket, forum, chat	
Price Indication (*)			◇	?	△	△	▽

* please refer to article text for explanation.
** due to nature of security products *public* support might be limited
*** for further explanantion please refer to article text.