

特点

- 密码
 - AES
 - DES/3DES
 - SNOW 3G
 - SEED
- 模式(支持所有块密码)
 - ECB
 - CBC
 - CFB
 - CTR
 - OFB
- 散列
 - 通过SHA-512的MD5和SHA-1
- MACs
 - CMAC
 - HMAC
 - XCBC
- 由美国国家标准与技术CAVP(密码算法验证程序)授权
- 资料库所针对常见的安全协议包括:
 - VPN – IPsec, SRTP和SSL
 - Wi-Fi, WiMAX, 3GPP, UMTS和LTE
 - DRM和条件访问
 - 政府和军事, 包括Suite B加密规范
- 支持阻塞和非阻塞模式(blocking and non-blocking modes)
 - 适应硬件核的卸载
- OS Agnostic
 - 可移植性的编写
 - 针对的操作系统– Linux, Windows Mobile, VxWorks, WindRiver, iTRON
 - C源代码的授权

ESS-01是依利浦系安全设计(ESA), 它是嵌入式应用提供一套全面安全软件的一个组成部分。ESS-01有一套完整的对称加密算法库, 例如AES,3DES, 散列函数SHA-1, SHA-2和密钥散列如HMAC/SHA-1。

这个库支持用硬件取代软件模块, 有益于设计者从系统上卸载内核, 或者使用一套全软件方案, 如果处理器的计算能力足够支持要求的通量。这个库的3.1版支持额外算法, 减少堆栈的大小并提高可移植性。

概述

ESS-01是依利浦提供的依利浦系安全设计的一部分。通过促使ESA的对称加密有效率的实施, 开发人员可加速产品的上市时间, 满足他们的总体性能目标, 并避免出现安全漏洞。

此库的3.1版支持额外的对称算法, 减少堆栈的大小并提高可移植性。依利浦将会继续支持那些使用依利浦系2.1版的客户直到3.1版发布一年以上。

Class	Function	Notes	Standard(s)	
Symmetric Ciphers	AES DES 3DES SEED CAMELLIA CAST5 SNOW 3G	Ciphers are implemented with ECB interfaces only. Wrappers are required to achieve chaining modes UEA2	FIPS-197 FIPS 46-2 FIPS 46-3 TTAS.KO-12.0004/R1 (SEED) RFC 3713 (Camellia) RFC 2144 (CAST5) TS 35.201 V7.0.0 (2007-06)	
	CBC CFB OFB CTR	Basic Chaining Modes		
	XTS	XTS (XEX) modes	IEEE 1619	
	Key Wrap	NIST Key Wrap	NIST – November 2001 RFC 3394	
	CMAC	NIST CMAC	SP-800-38B	
	XCBC	XCBC MAC Support 1 and 3 key mode	1 Key FFC 3566	
	CCM GCM	Encryption and authentication mode	SP-800-38C SP-800-38D	
	One-Way Hash Functions	MD5 SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 SNOW 3G	Hash algorithms provide hash only UIA2	RFC 1321 FIPS-180-3 TS 35.201 V7.0.0 (2007-06)
		HMAC	Hash based MAC	FIPS-198
		RNG/PRNG	System PRNG (/dev/urandom) ARC4	ARC4 can also be used as a cipher SSL

概述 – 续

ESS-01被设计成一种便携式库能够面向目前使用的所有嵌入式环境，包括 Linux, Windows Mobile, VwWorks, iTRON和 WindRiver。

当在许多微控制器和NPU现在已经拥有嵌入式加密核时候，这个资料库还支持硬件卸载，可以大大加快密码系统的吞吐量。

编码标准和示例

依利浦的编码标准是制订来确保客户的市场要求如汽车和医疗应用得以方便的使用这套资料库。使用的测试工具包括依利浦的半导体IP核所使用的FIPS测试向量，以确保核和软件库的相互操作。测试严格的遵守第三方测试实验室根据NIST CAVP验证的许可管理规范。

依利浦的网站上提供了两套示例。一套示例说明了散列算法如SHA-1，另一个侧是加密函数如AES。

依利浦系安全设计(Ellipsys Security Architecture)

下面所显示的依利浦系安全设计的图片由5个不同的产品组成，包括对称和非对称加密技术原语，安全引导，SRTP，Linux的IPsec和DTCP堆栈。

该设计提供了一个定义完善的，统一的API，该API结合了行业标准PKCS#11，其依利浦系的扩展能力支持第三方应该软件。客户可以配置依利浦系，和在硬件和软件安全基元之间进行选择，并能实现平台安全元素如安全启动和密钥管理。

在使用依利浦的硬件时，提供多种使用模式支持单一的加密甚至还提供先进的数据包处理引擎。

依利浦系安全设计也可适应用于板支持数据包(BSPs)的硬件shelf处理器的卸载，这些可以由依利浦编写，也可以由客户自己编写。

依利浦系的代码具有高便携可移植性，并有C源代码的许可。依利浦系安全设计如下图所示。

订购信息

- 提供高度可移植的源代码格式，ESS-01支持即时许可。
- 下表列出ESS-01的两套授权选择:

Order Code	Functionality
ESS-01-AES	AES cipher only (all modes)
ESS-01	All ciphers and hashes listed above

