“网安密+”端到端数据加密

安全技术白皮书

云数据安全方案

网安卫谷

浙江网安卫谷科技有限公司

目录

变更记录

版本	更新内容	更改人	更新日期
1.0	初版	Racy Yang	2017-09-26
1.1	增加 0054 相关内容并更新	Sandyen Qiu	2018-04-12
1.2	增加浏览器支持内容	Racy Yang	2019-08-17
1.3	增加国家密码法以及相关能力更新	Sandyen Qiu	2019-10-12
1.4	更新应用集成步骤说明	Sandyen Qiu	2024-11-7

1. 摘要

越来越多的企业和组织希望他们的沟通协作系统、业务流程系统能够被移动设备用户所访问，随着云计算的发展，SaaS 服务也逐渐被中大型企业，包括央企所接受。在充满安全挑战的环境中，企业从**信息化**走向**移动化**的同时，在移动互联网+的时代**安全化**已经成为企业在信息领域的头等大事。从单个应用到多个应用，到整体协作办公， 在移动化+云的过程中已经打破了原来的“安全边界”，从相对安全的“内网“（防火墙）进入了一个更为复杂的、不安全的互联网环境。这就要求企业建立/使用可信的安全服务，从确保单个应用到多个应用数据安全，最终推动企业安全的移动办公生态。” 网安密+“致力于为企业以及应用厂商提供可信的安全加密服务平台，为企业打造安全可靠的协同办公环境保驾护航。

2. 云安全面临的安全挑战

如今的互联世界依赖于任何地方、任何时间、任何设备上的数据可访问性。云服务和应用程序的速度和敏捷性是现代互联成功的核心。因此，这些固有的好处迫使组织将其部分或全部应用程序或基础设施迁移到云上。事实上，一些行业专家估计，到 2020 年，多达 83%的企业工作负载将迁移到云端。

随着企业开始转向云计算，互联网的安全问题越来越被关注，云服务的安全，特别是企业数据在云上的安全成为企业 CIO 考虑的首要问题。云服务、应用通过共享资源给企业带来极大灵活性，降低成本的同时，由于其自身的特点，也引入了较多不确定性，比如数据被共享（Facebook 事件），服务被黑客攻击导致数据泄漏，云服务商内部员工引起的数据泄漏等等。

云供应商虽然为用户的数据提供了一层基本的安全性。但是，从数据的机密性、完整性、访问控制等来说，远远不够。无法很好的防止各种类型的攻击，包括密码猜测攻击和中间人攻击，内部攻击，肩膀冲浪攻击和网络钓鱼攻击。以下列出了云中存在的安全挑战：

机密性：云中可能存储了大量敏感数据。这些数据必须具有额外的安全层，以减少破坏和网络钓鱼攻击的可能性; 这可以由组织来定义并完成。但是，作为预防措施，数据机密性应该是敏感材料的最优先考虑事项。

完整性： 在云环境中，应始终保持数据完整性，以避免任何固有的数据丢失。除了限制访问权限之外，对数据进行更改的权限应限于特定人员，以便在以后阶段不存在广泛的访问问题。

网络传输：由于互联网的开放性，以及移动化的办公方式逐渐成为大家的习惯，也就是企业数据会大量的在互联网上传输，因此在传输过程中如何确保企业数据不被黑客窃取，成为企业数据上云安全的重要一环。

云存储：企业数据作为重要资产，通常需要长时间的保存，以便后续的查询、审计等。数据在云端长期保存必将引起巨大的安全风险，云服务任何一次的安全事故对企业来说都将是灾难性的，不可逆的。

数据保护和滥用：当不同的组织使用云存储其数据时，通常存在数据滥用的风险。为了避免这种风险，迫切需要保护数据存储库。要完成此任务，可以使用身份验证并限制对云数据的访问控制。

访问：从长远来看，有关数据访问和控制的数据安全策略至关重要。授权数据所有者必须提供对个人的部分访问权限，以便每个人只获得存储在数据集市中的部分数据的所需访问权限。通过控制和限制访问，可以提供许多控制和数据安全性，以确保存储数据的最大安全性。

违规：云数据因为各种原因被泄漏的事件时有发生。除了黑客可以破坏云中的安全参数，并窃取可能被视为组织机密的数据。相反，违规可能是内部攻击，比如云服务商运维人员出卖、泄漏企业数据；企业员工因离职带着企业数据等。

3. 国家政策法规

“棱镜门”事件后的全国各行业国密化改造推进。2018 年 2 月，密标委发布了 GM/T 0054-2018 《信息系统密码应用基本要求》（简称国密 0054 标准），对信息系统中如何应用密码提出了基本要求，是当前指导、规范和评估信息系统中的商用密码应用的

标准依据。在 2019 年 5 月正式发布的等级保护 2.0（《网络安全等级保护基本要求》GB/T 22239-2019）内多次有明确的数据加密要求：

云计算安全扩展要求控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	基础设施位置	1	1	1	1
2	网络架构	2	3	5	8
3	网络边界的访问控制	1	2	2	2
4	网络边界的入侵防范	0	3	4	4
5	网络边界的安全审计	0	2	2	2
6	集中管控	0	0	4	4
7	计算环境的身份鉴别	0	0	1	1
8	计算环境的访问控制	2	2	2	2
9	计算环境的入侵防范	0	0	3	3
10	镜像和快照保护	0	2	3	3
11	数据安全性	1	3	4	4
12	数据备份恢复	0	2	4	4
13	剩余信息保护	0	2	2	2
14	云服务商选择	3	4	5	5
15	供应链管理	1	2	3	3
16	云计算环境管理	0	1	1	1

安全计算环境控制点 / 要求项的逐级变化

序号	控制点	一级	二级	三级	四级
1	身份鉴别	2	3	4	4
2	访问控制	3	4	7	7
3	安全审计	0	3	4	4
4	入侵防范	2	5	6	6
5	恶意代码防范	1	1	1	1
6	可信验证	1	1	1	1
7	数据完整性	1	1	2	3
8	数据保密性	0	0	2	2
9	数据备份与恢复	1	2	3	4
10	剩余信息保护	0	1	2	2
11	个人信息保护	0	2	2	2

《中华人民共和国网络安全法》2017 年实施

- 根据信息安全行业共识，使用无资质的国际加密算法视同未加密明文处理用户信息
- 此行为违反《中华人民共和国网络安全法》第 42 条，拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

《GM/T 0054-2018 信息系统密码应用基本要求》2018 年实施

- 密评是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估的活动
- 关键信息基础设施不得**低于等保三级**

《中华人民共和国密码法》2019 年实施

- 要求使用商用密码进行保护的关键信息基础设施
- 面向公众提供网络信息服务或支撑**能源、通信、金融、交通、公共事业**等重要行业运行的信息系统或工业控制系统，其运营者应当使用商用密码进行保护，开展商用密码应用安全性评估”

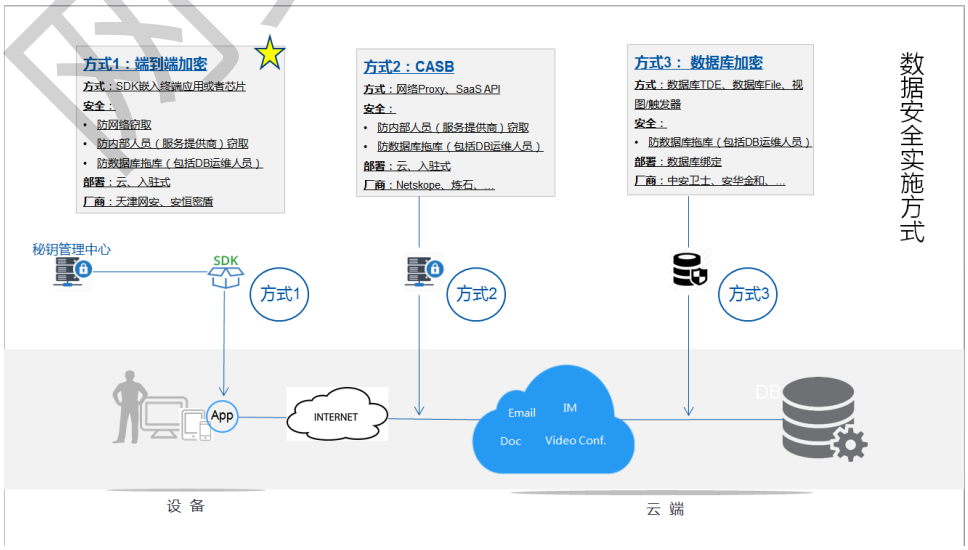
4. 安全解决方案

4.1. 业界安全方案比较

随着云应用的普及，云安全不再是空泛的概念和技术设想，已有众多厂商针对云的安全脆弱点以及安全需求开发出相应的产品并投入市场。本质上这些方案都是在某个切入点对数据进行加密以保护企业数据在云上的安全。根据切入点不同，一般有以下三种方式：

- **端到端加密**：从数据产生的源头进行国密加密，数据以密文的形式进入互联网传输，同样数据在云上以密文存储，只有接收方才能对数据进行解密
- **CASB**：数据在进入云服务器之前进行数据加密，这样数据在互联网上以明文形式传输，在云上以密文存储
- **数据库加密**：数据在进入数据库时对数据进行加密，也就是数据互联网传输过程以及在云上处理是以明文存在，只有进入磁盘（数据库）才进行加密

如上图所示，从数据的生命周期覆盖程度来讲，端到端加密方案是覆盖最为全面，从防网络窃取、防内部人员（服务提供商）窃取以及防云端数据被泄漏（数据库被拖库）。而数据库加密仅仅保护云

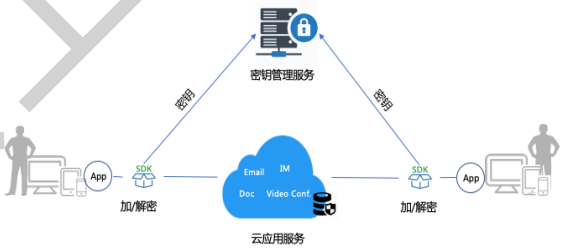


应用数据在数据库中的存储安全，CASB 虽然覆盖范围比数据库加密有所增加，但是无法很好的保护数据在互联网传输过程中的安全。因此，为了更好的保证企业数据安全，我们强烈推荐企业在应用上云过程中使用端到端加密技术，以便在数据在整个生命周期过程中得到更好的保护。

4.2. 网安云数据安全方案

4.2.1. 方案概述

网安密+，致力于解决企业在使用云服务过程中产生的安全问题，采用端对端的加解密数据安全方案，即数据从终端进入网络之前先进行安全加密，确保数据在网络传输过程中、云服务处理存储过程中都是被加密的，只有集成网安安全套件的接收终端才有解密的能力，实现用户数据在互联网传输以及云上存储的安全。企业加密数据和加密密钥分开独立存储的方式，确保了企业数据只能被企业授权的用户访问，其他任何人都无法查看企业信息。



产品从用户认证、密钥分发管理、数据加密等方面为企业的数据提供安全保驾护航：

- **防外部用户**： 企业外或已离职用户无法获取密钥，有效保证企业敏感数据的安全
- **防窃取泄露**：即使应用服务器遭受攻击后，企业敏感数据也因加密而无法阅读
- **防电信运营商**：防止企业敏感数据在网络（含境外电信数据网络）传输过程中被非法窃取后的泄露

- **防应用服务商**：防止应用服务提供商人员非法访问到服务器端存储的企业敏感数据引起的泄露
- **防云服务商**：防止云服务提供商运维人员访问到应用服务存储的企业敏感数据引起的泄露

产品是以第三方的形式独立于应用服务存在，为企业上云的应用提供完整的数据安全服务。系统分为两部分：一是密钥服务器（云）以集群化形式部署在中国网安高安全的“卫士云”上，提供高可用性、高扩展性的云服务（企业也可根据自身需求私有化部署），主要提供密钥的安全存储以及企业密钥的分发和管理；二是安全套件以 SDK 的形式集成在终端应用中，确保应用数据提供国密加解密能力。安全套件根据用户信息从服务器获取用户密钥，为应用提供国密服务。

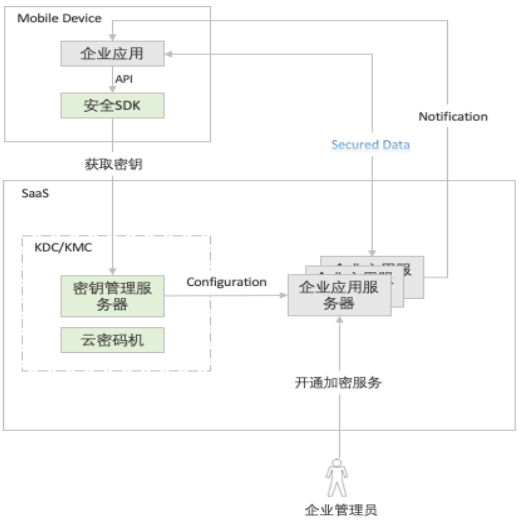
注：以上主要介绍基于互联网的常见的应用场景，保证数据经过国密加密后只有通信双方可以获取数据的明文。从广义的角度，此方案同样适用于从端到服务器的国密加密保护，该场景下数据在应用服务器上的安全需要应用服务提供者确保解密的数据不落地，落地的数据需要经过国密加密。

4.2.2. 系统结构说明

网安密+云数据安全平台主要有三部分组成：

安全套件(SDK)：集成在企业应用 App 中为应用提供安全能力

密钥管理服务器(KDC/KMC)：以云服务的形式提供企业密钥的分发以及管理

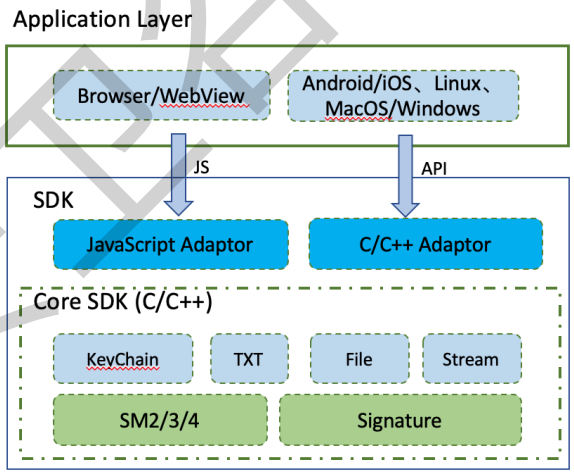


云密码机：基于真随机数生产加密所需的密钥以及各种国密局认证的加密算法能力

上图所示，网安密+产品各个模块所处的位置，与企业应用之间的关系，以及系统之间数据流向。密钥管理服务器以不侵入企业应用服务器的方式，可以直接使用企业应用服务器开放的 API 快速形成集成，使企业应用快速形成国密安全能力。

4.2.3. 安全套件（SDK）

安全套件以 SDK 的形式为应用提供国密安全能力，应用开发者不需要有任何密码知识，也不用关心加解密过程，根据需要直接使用加解密 API 接口即可。安全套件以“绿色”软件的形态存在，完全对应用层保持透明。



如图所示，安全套件根据不同的应用提供对应的 API 以供应用使用，最大程度降低应用集成成本。安全套件内部分为核心库和适配（Adaptor）部分，核心部分考虑到执行效率以及安全性以 C/C++实现，适配层为 web 应用提供了 JavaScript 接口以及为 Native 应用提供了 C/C++接口。安全套件主要提供能力如下：

- **密钥链(KeyChain)**：密钥的产生、获取以及采用基于密码保护机制所需要的密钥链对密钥进行保护，为了安全性，用户密钥不存储在终端设备中
- **文本消息（TXT）**：提供基于文本消息的加解密能力，一话一密
- **文件（File）**：提供基于文件的加解密能力，一文件一密钥。对于超大文件（>1GB）采用分片处理的能力

- **流（Stream）**：提供基于音、视频流的处理，实际验证结果，加密后的音视频无衰减，用户无感
- **独立认证（可选）**：提供独立的二次身份认证，确保获取密钥的用户身份真实可信。二次身份认证支持短信、邮件等常用方式

注：众所周知，浏览器插件本身存在一定的安全隐患。区别于常用的安全方案（包括网银），网安密+浏览器安全套件采用无插件方式，也就是用户在使用过程中无需安装插件，可以直接获得国密加解密能力。

5. 产品说明及特点

5.1. 产品简介

网安密+采用商密算法对企业核心业务数据进行端到端的二次加密，通过对用户认证、密钥分发管理、数据加解密等重要环节的严格把控，实现了企业信息数据从终端、通信链路到云服务平台三位一体的安全防护，有效地保证企业核心业务数据在云端传输以及存储的安全性。

使用网安密+，由原来的一把钥匙变成两把钥匙。在如企业微信等云服务提供商的服务器上只存放加密后的数据，在密钥服务器上只存放密钥，从物理上实现了加密的企业数据和加密密钥的分开独立存储，实现两把锁分离存放。而集成了安全套件（SDK）的客户终端只有同时拿到了密钥和密文数据才能解密，无论是云服务提供商还是密钥服务器上的数据都无法单独解密数据，大大增加了黑客破解整个企业敏感信息的难度，提高了数据的安全性。

使用网安密+，不仅解决了企业敏感信息在互联网云端存储的安全问题，保证数据的安全性，还大幅减少了相关的沟通，建设和运维成本。只需要管理员开启后，企业即进入加密模式 ，整个加密过程不影响用户的正常操作，完全做到无感操作。

5.2. 产品特点

身份认证：产品独立于云服务提供商，自建了一套身份认证机制。即使是经过云服务提供商验证通过的企业用户，任何未经企业管理员授权的用户、伪造企业授权的用户和身份信息失窃后的入侵都将被独立的多重身份认证拒之门外，保障企业内使用加密服务用户的合法性、真实性和有效性。

数据加密：数据已经成为政企核心资产和经济发展命脉，无论是国家安全、经济发展、社会生活中已起到关键作用，因为数据的高价值所以也成为了攻击者的重要目标之一。网安密+采用 SM2/4 高强度国密算法对企业核心业务数据进行端到端加密保护，所有的消息内容只有收发者才能查看。在数据传输、存储、处理、交换等的过程中，保障数据生命周期安全，持续提升企业数据安全保障能力。

而安全套件 SDK 在密钥获取的过程中，为防止中间人攻击篡改，全程采用 SM2、SM4 加密保护及 SM2 签名验证，即使截获链路数据也无法解密篡改， 保证密钥数据的安全性。

密钥可控：密钥管理是数据安全的基石！网安密+的密钥由国密密码机随机产生，具有绝对唯一性。企业管理员随时或定期更新密钥，实现对企业密钥的完全自主可控，

而服务器对密钥更新进行的审计，保证更新操作的可追溯性。安全套件 SDK 对密钥分多层使用，层层保护，安全可靠。而对于对本地密钥，则通过多种算法进行强保护，保证本地密钥的安全性！

5.3. 产品优势

密码机： 提供真随机数，密钥全生命周期管理，军工级密钥管理和保障标准要求，获得国密局商密认证证书；符合国家密码设备合规性要求

商密算法：国密局认证，保证算法的自主可控，对称和非对称加密算法对数据进行强保护；符合国家密码算法合规性要求

全程加密：密钥获取过程全程加密，采用非对称算法和对称算法，保证数据的安全性，即使截获链路数据也无法解密；密钥和内容均采用加密保护，安全无遗漏

多重认证：独立提供多种用户认证方式；按需定制二次认证方式，灵活又安全

海外加速：使用全球分布的 DSA（动态网络加速）技术 ，全面助力海外业务，助力一带一路

全平台：支持主流的移动端、浏览器和 PC 端平台， 提供动态库和静态库，主要有 Android、iOS、MacOS、Windows、Linux，Chrome、Firefox、Safari 、Edge 等主流浏览器

5.4. 应用领域

网安密+为企业提供端到端加解密能力，可广泛使用于即时通讯、语音/视频会议、安全邮件、智能家居、互联网汽车、云盘、物联网等领域。同时，网安密+可以基于公有云、混合云、私有云进行部署，可以满足跨国企业各分支机构的互联互通需求，同样适用于各类企业一带一路发展布局，既能满足海外用户的使用要求，又有国密级加密保证。

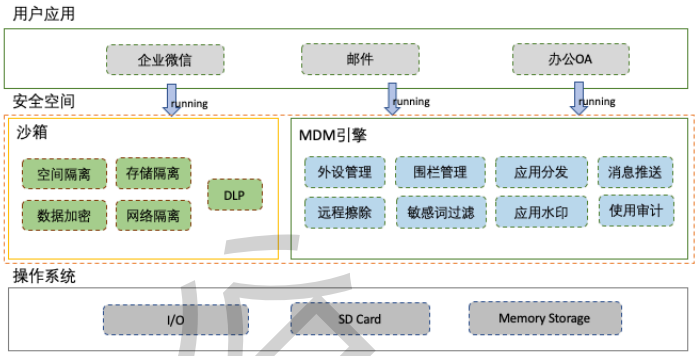
5.5. 应用生态

随着企业信息化的逐步完善，以及各种新型技术的发展，企事业单位逐步上线了大量的应用系统以适应移动互联网的发展。用户在使用信息时的应用场景也变得越来越复杂，需要在多个应用中切换，分享信息来完成某个特定的应用场景。比如把邮件收到的文件以安全的方式分享到企业即时通信的群中，再比如把企业即时通信的文件以安全的方式上传到企业网盘中。为了避免信息孤岛，各种应用之间的信息转换，传递就变得不可避免。这就要求信息在保证安全的情况下需要通过各类应用之间的共享，分发协作来完成。

网安密+产品是中国网安基于各种企业应用场景，打造的围绕身份（密码）来解决企业在应用上云过程的安全问题。平台采用了以企业和用户身份为中心的密钥分发体系，在做到每个文件拥有独立的密钥，并且文件只需加密一次，即可根据不同的使用场景， 在不同的应用之间安全的分发。保证了对应用使用者的透明、无感，也就是在不改变用户体验的情况下保证了企业管理者对数据安全的担

心。也打破了安全必须以牺牲用户体验为代价的定律，大大解决了企业安全类产品使用率低的问题。

网安密+帮助企业解决了企业应用上云的安全关切，然后移动终端由于其便利性，不确定性带来的“端”上的安全同样给企业数据带来巨大的安全威胁。比如个人信息和企业信息交叉、终端上不安全的应用App、不安全的移动网络（WIFI）、数据被以各种方式分享到社交网络等等。从数据安全生命周期来说，企业需要对企业数据的使用场景做一定限制，以防止员工有意或者无意的情况下造成的数据泄露。如下图所示，网安卫谷针对这类应用场景，开发了集安全沙箱以及 MDM 引擎为一体的安全空间，为企业用户在移动终端上隔离出专有的办公桌面，该空间能有效限制用户行为，形成类似企业内网 PC 终端的隔离效果。



安全空间由两个核心模块组成：

沙箱：提供独立的类似双系统的用户隔离空间以及用户体验，所有应用在无需修改的情况下安装在沙箱内，直接拥有沙箱提供的安全能力，包括本地数据国密加密、安全的网络（VPN/VPDN）、与个人数据隔离以及防数据泄露等能力。

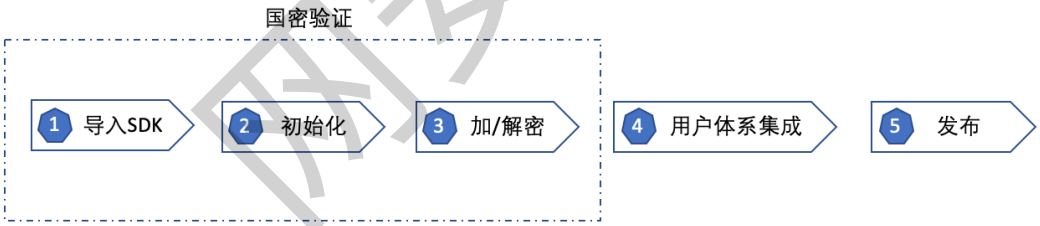
MDM 引擎：提供对移动设备全方位的安全管理，外设管理控制应用所能访问和使用的外设，如相机、WIFI、Bluetooth 等；应用敏感词限制可以限制敏感性是否可以发送；应用水印可以给所有应用提供水印能力，防止截屏、被拍照引起的数据安全泄露...

6. 产品集成

网安密+在考虑安全性的前提下，充分考虑到应用系统的集成需求，加密系统不改变既有应用用户体验，可以让应用快速集成来获取商密能力满足国家的合规要求，主要体现在：

- 全平台支持，支持所有主流 OS（包括嵌入式），原生应用，H5 和主流浏览器
- 低侵入性，以应用为中心，应用系统不产生外部依赖（SDK 需要嵌入应用）
- 易集成，安全套件 SDK 绿色可靠，不依赖平台特性，提供平台友好的 API，正常集成工作量小于一天
- 用户体验：不改变应用用户体验

集成流程如下图所示：



1. 在应用的工程中导入加密SDK（绿色，无其他依赖）
2. 应用登录完成后初始化SDK
3. 在应用数据读写（I/O)时对数据加解密 （完成这步后可以做端到端加密测试）
4. 应用服务器提供API供加密系统做用户对接（认证、退出等）
5. 正式发布

7. 部署方案

网安密+支持 SaaS 部署和入驻式部署，整套系统可以根据企业的业务系统现状和要求采用不同的部署方案。服务主要包含密钥分发服务（KDC）、密钥管理服务（KMC）、物理密码机（可替换云密码机）以及数据库服务。同时需要辅助服务有：邮件发送服务（SMTP）或者短信发送网关，辅助服务属于可选服务，只有在开启二次认证的情况下是必须的。

7.1. SAAS 服务

产品以云服务的形式给云应用或者企业入驻式应用提供安全加密服务能力，无需企业部署建设任何服务器，企业只需按照自身的需求随时购买 License 即可。企业自有的业务系统（云或者入驻式）可以直接对接网安的云数据安全加密服务平台，使用其提供的 SaaS 服务。这种部署模式可大幅节省建立私有沟通和协同平台的建设和运维费用。网安密+服务集群化部署于中国网安高安全“卫士云”上。卫士云通过国家等保三级资质认证，有专业的运维团队提供 24 小时的服务。 基于云的云数据安全服务具有以下能力：

- 7x24 小时的运维、监控保障
- 密钥长期保存（>10 年），确保企业信息可被追溯审计
- 海外加速，全球分布的 DSA（动态网络加速）技术
- 云密码机提供密钥以及密码服务
- 短信网关或 SMTP 服务（二次认证）

7.2. 入驻式部署

对于安全性要求较高的企业，基于高安全性的要求，可以私有化部署加密服务以及密码机，以便做到自主可控，私有化加密密钥。产品支持企业自建服务器部署， 也就是在企业自己的环境中部署加密服务以及密码机等，进行独立运维。

7.2.1. 推荐配置

服务器用途	服务器配置	数量（台）	备注
Keepalived+LVS	2 核 4G 内存 100G 存储	2	
KDC/KMC 节点	2 核 8G 100G 存储	2	
Redis/MySQL 节点	4 核 16G 机器 400G 存储	3	
密码机	SJJ1866	2	

说明：该配置以高可用，可扩展，高稳定性为基本原则，基于低延时，高并发的要求。原则上支持不少于 10 万用户同时在线的能力建设。

7.2.2. 最小配置

服务器用途	服务器配置	数量（台）	备注
All in one	8 核 16G 机器 200G 存储	1	
密码机	SJJ1866	1	

说明：该配置不考虑高可用，高稳定，所有服务采用单点资源提供服务。原则上支持不少于 2000 用户同时在线的能力建设。

8. 成功案例

8.1. SAAS 加密服务

网安密+是腾讯在企业微信 SaaS 版本第三方加密服务领域唯一合作伙伴，为政企用户提供专业的企业微信第三方加密服务。目前开通使用网安密+加密服务的世界 500 强企业：

8.2. 入驻式加密服务

广东省“数字政府”政务云平台汇集处理全省的电子政务业务。海量数据资源高度集中形成价值高地，大量的政府公共敏感数据、个 人隐私数据等安全亟需防护，开放的互联网访问方式加剧了平台信息泄露的风险，催生了更高等级的安全防护需求。密码是保障信息安全 的核心支撑技术，通过身份认证、数据保护、资源隔离、可信服务等 手段，可有效保障系统、数据的生命周期安全。

9. 附录

9.1. 技术指标

指标类型	指标项	具体情况
功能指标	通信模式	支持客户端之间单聊和群聊通信加密
	企业成员管理	支持添加、获取、删除加密企业中的成员，对其进行身份认证确认
	企业加密服务验证码管	支持对企业加密服务验证码的设置、获取和删除功能
	加密服务验证方式管理	企业可选择关闭验证或者开启短信、邮件、短信&邮件验证
	密钥管理	支持更换密钥轮换周期
		支持强制更新企业当前密钥
	客户端加密传输功能	支持客户端之间聊天文本/图片/文件/语音/视频加密传输功能
	历史消息	支持对历史聊天信息的解密功能
	收藏	支持对个人收藏的加密存储、解密和转发功能
性能指标	服务用户能力	支持 3,000,000 用户同时在线，并可线性扩展
	服务响应能力	支持每秒 200+并发(RPS<200)
	加解密能力	10M 数据，所有平台耗时<700 毫秒
	客户端操作系统	Android 5.0 及以上、iOS 8.0 及以上 MacOS 10.9 及以上 Windows XP & Windows 7 & Windows 10 Linux（CentOS 6.7 及以上） H5、小程序以及主流浏览器 Chrome、Safari 等
	加解密	消息加解密 100%成功
	客户端 SDK	支持 SM2、SM3、SM4 密码算法

加解密指标	密钥管理端	支持 SM2、SM3、 SM4 密码算法