格尔签名验证服务器SRJ1312

产品白皮书

上海格尔软件股份有限公司

2017年3月

保密事宜：

本文档包含上海格尔软件股份有限公司的专有商业信息和保密信息。

接受方同意维护本文档所提供信息的保密性，承诺不对其进行复制，或向评估小组以外、非直接相关的人员公开此信息。对于以下三种信息，接受方不向格尔公司承担保密责任：

1） 接受方在接收该文档前，已经掌握的信息。

2） 可以通过与接受方无关的其它渠道公开获得的信息。

3） 可以从第三方，以无附加保密要求方式获得的信息。

上海格尔软件股份有限公司

上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼

URL: http://www.koal.com/

目 录

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL: http://www.koal.com/

1 前言

1.1 产品背景

随着网络的快速发展，网络应用已经成为一种趋势，如电子政务、电子商务、网上办公等，越来越多的重要信息在网络中流转，网络应用中认证机制弱，明文传输等安全隐患严重阻碍了信息化的发展，如何保护这些数据的流转安全是网络应用面临的一个重要问题。目前最高强度的技术是采用基于 PKI 技术的电子签名和验证的安全技术，它可以解决网络应用身份认证以及数据完整性，不可抵赖性等问题，并得到广泛的认可。其核心的安全特性如下：

1. **身份认证：**与传统的信息交换不同，参与网上信息交换的各方没有实际见面，任何一方都有被冒充的可能，所以安全应用系统必须采用某种机制，使能够确认对方的身份。
2. **数据保密：**在许多应用中，信息的内容是需要严格保密的，但是在网络上，网络侦听技术使数据的获取变得十分容易，因此对信息的加密是安全应用系统重要的特点。
3. **数据防篡改：**由于网络的公开特性，使得信息提供者以外的人修改信息成为可能。如何防止他人篡改信息是安全应用系统需要解决的一个重要问题。
4. **操作防抵赖：**在信息提供过程中如果一方在确认信息操作后又抵赖，将对应用系统的使用造成很大的损失。安全应用系统必须提供某种技术手段，以便应用系统能对信息的提供进行确认。

以上 4 点是 PKI 应用支撑产品的核心功能，与市场上常见的服务器密码机（通常称为"加密机"）有部分重叠，但签名验证产品提供的是更侧重于应用的服务接口，因此，签名验证产品除了提供基本的签名，验签，证书验证等功能之外，还应该对业务特性，比如文本编码，业务流水，文件处理等各方面进行支持。格尔签名验证服务器正是这样一款针对应用设计的 PKI 安全支撑产品。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL: http://www.koal.com/

1.2 名词解释

- ✧ 证书认证机构（Certificate Authority）：一个产生和确定公开密钥证书的可靠和可信的第三方机构。它发行数字证书并确保证书的可信性，或证明一个用户和它们的公共密钥的身份。认证机构也可以为实体产生和确定密钥。习惯上又称作认证中心（CA）。

- ✧ 数字证书（Certificate）：数字证书就是互联网通讯中标志通讯各方身份信息的一串数字，提供了一种在 Internet 上验证通信实体身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个由权威机构——CA 机构，又称为证书授权（Certificate Authority）中心发行的，人们可以在网上用它来识别对方的身份。数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。

- ✧ 数字签名（Digital Signature）：数字签名（又称公钥数字签名、电子签章）是一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，用于鉴别数字信息的方法。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。
- ✧ 数字信封（Digital Envelope）：数字信封是公钥密码体制在实际中的一个应用，使用加密技术来保证只有规定的特定接收者才能阅读信息的内容。
- ✧ SM2：国家密码管理局颁布的商用密码非对称算法，用于取代 RSA 算法，SM2 算法相关的国标规范已经全面推行。

- ✧ SM4：国家密码管理局颁布的商用密码对称算法，用于取代美标的 DES，AES 等算法。

- ✧ SM3：国家密码管理局颁布的商用密码杂凑算法，用于取代美标的 MD5，SHA1 等算法

- ✧ SM1：国家密码管理局较早时候颁布的商用密码对称算法，用于取代美标的 DES，AES 等算法，可以被 SM4 取代。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL: http://www.koal.com/

- ✧ LDAP：(Lightweight Directory Access Protocol) 是一种轻量级的目录存取协定，提供客户从各个角落连接到目录服务器中。本手册中专指 CA 用于发布证书及黑名单的 LDAP 服务。
- ✧ 黑名单：通常所说的 CRL（Certificate Revoke List），因时间或者安全原因被废除的证书列表，一般发布在 LDAP 上。
- ✧ PKCS#7：一种国际通用的数据封装格式，用于规范数字签名，数字信封的二进制数据组织。

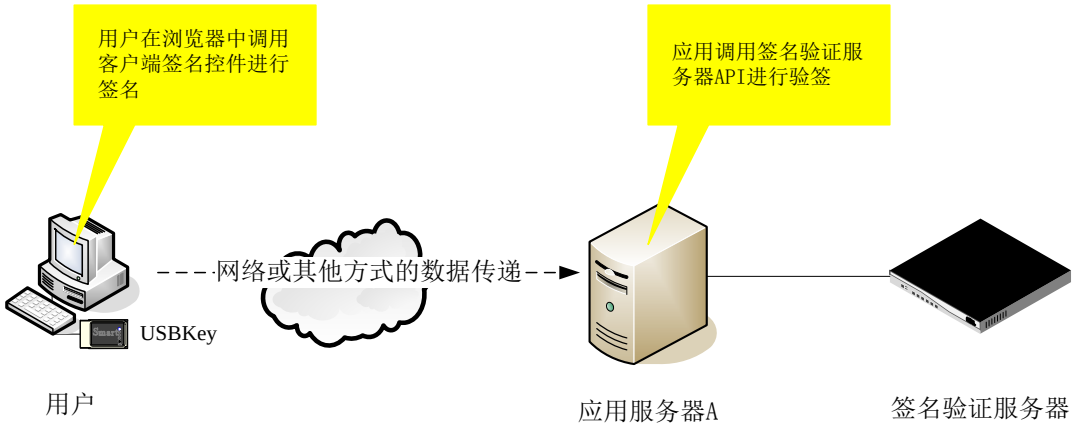
2 产品概述

格尔签名验证服务器最初版本发布于 2003 年，是一款提供数字签名/验证签名服务的硬件产品，该产品可以被广泛地应用在网上银行/证券/保险等电子商务和电子政务活动中，用于确认用户身份、保障信息完整性、保证交易的不可否认性（抗抵赖）。该产品的设计路线不同于服务器密码机产品，侧重于与应用结合的方面，并形成了自身的特色。同时，伴随着商用密码技术的不断发展，陆续获得过多个商用密码型号，在国家陆续发布 SM2，SM3，SM4 等算法及相关规范后，该产品于 2013 年获得最新的商用密码型号为 SRJ1312（高性能签名验签服务器）。

签名验证系统由签名验证服务器（硬件），服务端 API 和客户端签名控件组成，典型的使用场景如下：

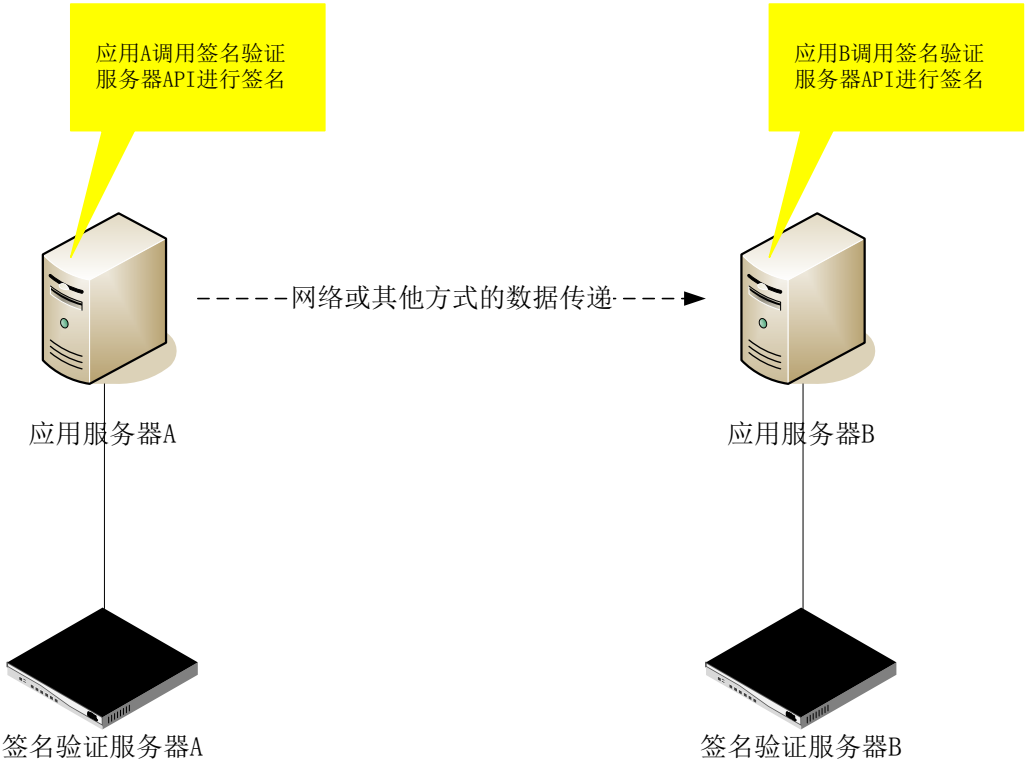
场景 1：客户端（浏览器端）签名，服务端验签——比如网银的客户在进行转账时，在浏览器端调用 USBKey 进行签名，由网页将签名结果提交到应用后台后，应用调用签名验证服务端 API 进行验证签名。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL: http://www.koal.com/



图表 1 客户端签名，服务端验证

场景 2：不同的服务之间的签名和验证——适用于多个大型机构不同应用之间进行相互的数据签名和验证。



图表 2 服务端相互签名，验签

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL: http://www.koal.com/

3 产品功能

功能	说明
数据签名功能	提供普通格式，PKCS#7 Attach/Detach 等多种格式的数字签名功能
签名验证功能	提供普通格式，PKCS#7 Attach/Detach 等多种格式的数字签名验证功能
文件签名功能	对文件提供数字签名功能（在 API 中计算摘要）
文件验证签名功能	对文件提供数字签名验证功能（在 API 中计算摘要）
数字信封功能	提供 PKCS#7 格式的数字信封加密和解密功能
证书有效性验证功能	提供黑名单/在线证书验证等多种方式的证书有效性验证
时间戳功能	支持 PKCS#9 SigningTime
业务流水号功能	支持业务系统在调用时传入相关的业务流水号，并记入日志，便于业务系统后期对账、维护使用。
动态黑名单功能	系统可以自动更新黑名单、动态更新，不需要重新启动服务
多签名证书功能	可根据不同的签名证书创建多个服务实例，由调用者选择使用。
多证书链功能	可同时配置多条证书链，验证不同 CA 的用户证书
获取证书信息功能	提供证书解析功能，获取证书中的任意主题信息以及扩展项信息
多种证书支持功能	支持 CFCA、BJCA，SHECA 及符合国家密码管理局相关规范的 CA 中心数字证书

系统备份恢复功能	系统可以备份当前所有配置，保证系统瘫痪时的快速恢复
日志发送功能	系统将日志以 SYSLOG 的方式发送到指定服务器。
双机热备功能	高可靠性
自负载功能	支持在无外部负载均衡器的情况下，使用 2 台及以上的签名验证服务器组成一个自管理的集群。
网卡冗余功能	支持将两个网络接口聚合为一个，实现链路聚合
多种开发接口支持	客户端签名控件开发接口： Windows COM API Java API（封装 COM API） 服务端开发接口： Windows COM API Java API 语言无关的 HTTP 接口（以 HTTP 报文形式调用）

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL: http://www.koal.com/

4 产品型号

格尔签名验证服务器采用专用的设备硬件来保证密码运算的安全和效率，产品形态如下图所示（外观图仅做参考，具体外观及接口以实物为准）：

图表 3 产品形态

	3000	3200	6400	6800	8800
设备高度	1U	1U	2U	2U	4U
网络接口	6*1000M	6*1000M	6*1000M	8*1000M	8*1000M
电源数量	1	1	1（可选配 2）	2	2
RSA(1024 位)签名	500 次/秒	2000 次/秒	5000 次/秒	10000 次/秒	30000 次/秒
RSA(1024 位)验签	1000 次/秒	4000 次/秒	8000 次/秒	15000 次/秒	30000 次/秒
RSA(2048 位)签名	150 次/秒	500 次/秒	1500 次/秒	5000 次/秒	20000 次/秒
RSA(2048 位)验签	1000 次/秒	2000 次/秒	5000 次/秒	10000 次/秒	30000 次/秒
SM2(256 位)签名	500 次/秒	1000 次/秒	2000 次/秒	8000 次/秒	30000 次/秒
SM2(256 位)验签	200 次/秒	500 次/秒	1000 次/秒	4000 次/秒	20000 次/秒

注：上述所有规格及参数若有变动，请以厂家提供的最终配置为准。

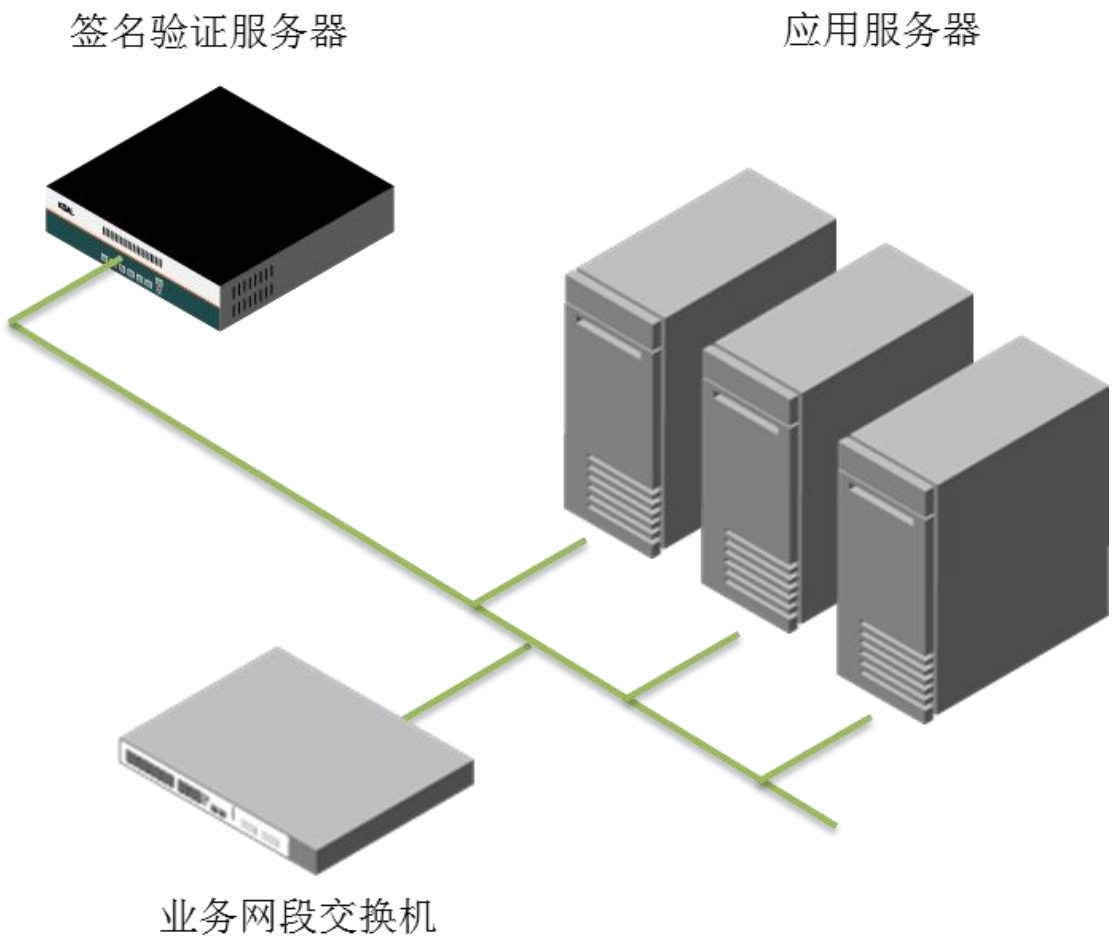
上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL: http://www.koal.com/

5 产品特点

- 完善的算法支持：支持商用密码算法 SM2/SM3/SM4，支持国际通用算法 RSA/AES/SHA1 等。
- 支持多种类型签名数据：支持原文数据签名、文件签名、哈希后签名及 PKCS #7 等格式签名数据的验证。
- 支持多种字符编码处理：支持文本数据在不同编码系统（UNICODE，GBK，UTF-8）之间的签名一致性。
- 支持业务流水号：运行应用在签名数据时传入相关的业务流水号，并计入日志，方便对账和历史数据查询。
- 支持多种证书验证方式：支持黑名单验证方式以及在线证书验证方式。
- 支持热备。系统可以进行双机热备，保证系统的高可用性。
- 支持自负载：支持 2 台及以上的设备，在无外部负载均衡器的情况下，组成一个自管理的集群。
- 支持网卡冗余：支持将 2 个网络接口聚合为一个接口，实现链路聚合功能。
- 支持多种开发接口：客户端提供 Windows COM API，Java 开发 API，方便应用的调用。
- 系统日志标准输出支持：通过标准的 SYSLOG 方式将用户日志发送到指定服务器。
- 备份恢复功能支持：系统具有备份和恢复功能，对于系统的数据和配置进行加密完全备份，能够快速恢复。
- 系统设置专用网络接口管理系统，系统关闭所有不需要的服务和端口（如 FTP、SSH 等），只保留服务端口，避免外界的攻击。
- 系统所有管理操作均采用 WEB 方式，操作简单方便。

6 产品部署

6.1 简单部署



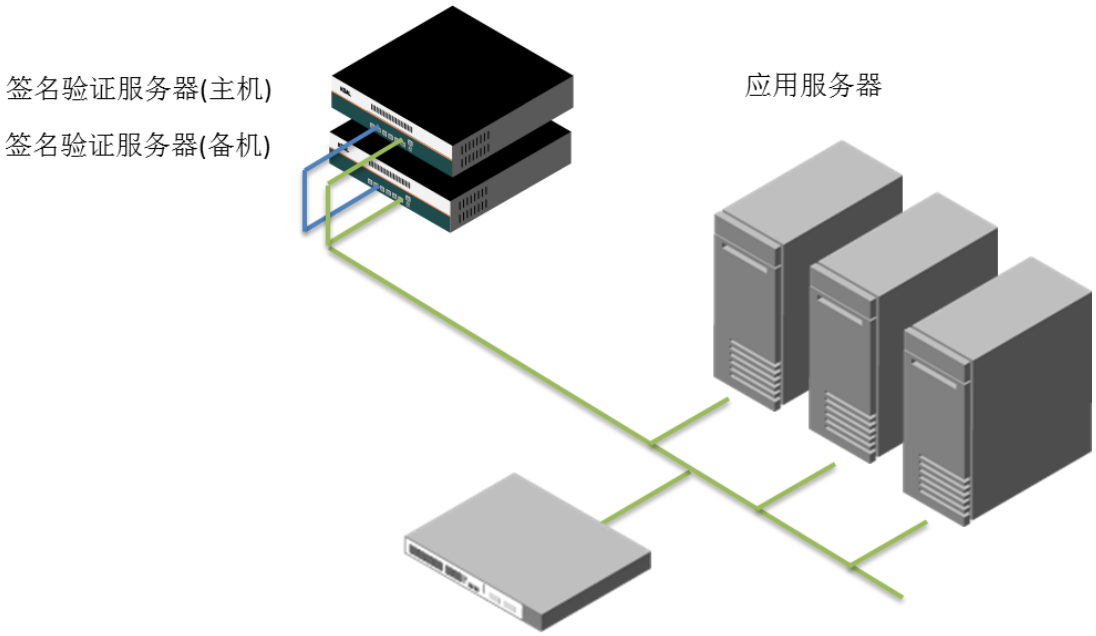
图表 4 简单部署

签名验证服务器一般采用与应用服务器并联部署的方式，可以同时为多个应用服务器提供服务。

如果需要开启签名验证服务器的黑名单下载或在线证书验证功能，还需要在网络规划上允许签名验证服务访问 CA 的 LDAP 服务器。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL: http://www.koal.com/

6.2 热备部署

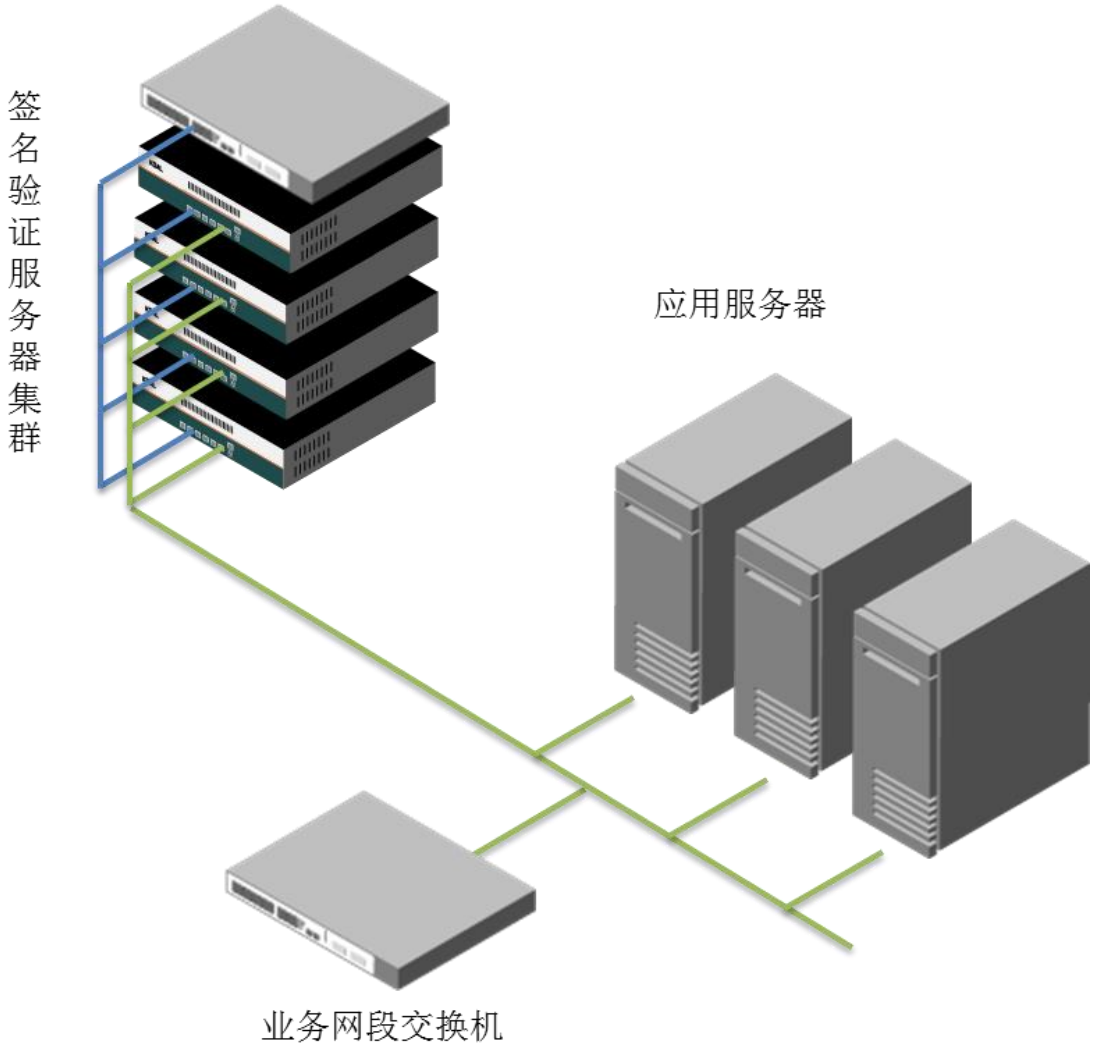


图表 5 热备部署

热备部署模式与简单部署方式类似，将主备机的业务网口都连接到业务网段交换机，然后再采用一根心跳线连接主备机的热备口即可。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL: http://www.koal.com/

6.3 自负载部署



图表 6 自负载部署

2 台及以上签名验证服务器可以组成一个自负载的集群，此时部署方式如上图所示，除了每台签名验证服务器的业务网口需要与应用系统相连之外，各台签名验证服务器的热备口应该能通过一个单独的交换机（或者 VLAN）进行相互通讯，进行集群所需的节点协商。

注：如果只使用 2 台签名验证服务器进行自负载，则可以不需要单独的交换机（或则 VLAN），只需要用网线直连热备口即可，此时的部署方式与热备模式相同。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL: http://www.koal.com/

7 产品证书

商用密码产品型号证书

（证书编号：SXH2013156 号）

单位名称：上海格尔软件股份有限公司

申报名称：高性能签名验签服务器

批准型号：SRJ1312 签名验签服务器

说明：证书有效期五年

国家密码管理局

2013 年 12 月 16 日

上海格尔软件股份有限公司

上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼

URL: http://www.koal.com/