MTS SmartService™安全概要

全套MTS SmartService工具帮助
用户快速了解测试设备的服务信息

简介

MTS系统公司承诺客户的数据和服务信息均受到最高级别的保密加护，相应的服务解决方案也必需能够保护客户数据的安全。本文简要介绍了MTS SmartService平台的系统安全特性与构架：

» 安全保密

» 物理构架与网络

» 业务的持续性以及灾难后恢复

» 监控

» 客户支持

近场通信的安全性

MTS SmartService平台基于近场通信(NFC)技术，在设备标签内植入了近场通信芯片，该芯片除了保存有一个特别的序列号之外不存储任何系统历史数据。

离线模式的安全性

使用MTS SmartService客户平板时，就如同用苹果iOS系统的隔空投送(AirDrop)一样方便快捷，只有与MTS现场服务工程师所持有的智能终端相匹配时，才可以进行类似固件升级、软件升级以及数据备份等离线操作。这些过程将使用低能耗蓝牙技术进行设备识别，安全Wi-Fi热点创建连接，使用以安全为目标的 HTTP 通道(HTTPS)进行数据传输，所有数据均采用256位SSL加密技术予以保护数据安全有效。

通讯的安全性

MTS SmartService客户平板具有在线备份和升级功能，该功能需要Wi-Fi连接，使用图形界面选择安全的网络连接完成设置与控制。

» 包含无线网络服务集标识(SSID)搜索、连接、断开、忽略等功能；

» 支持WPA2、EAP、专属门户的客户网络以及HTTP代理设置功能；

» 数据备份与更新基于256位SSL数据加密连接；

» 数据通信采用256位SSL/TLS AES加密；

» 不需要固件端口；

» MTS SmartService客户平板控制历史数据备份的全过程；

服务历史数据的安全性

为了防止服务历史数据在传输过程中被窃听或者被拦截，MTS采用了以安全为目标的 HTTP 通道(HTTPS)进行数据传输，数据采用传输层安全性(TLS)进行加密，保证数据的安全可靠。在网络或者服务器上的数据只有授权人员才能够访问，并且利用口令和认证令牌进行双重控制。MTS 将基于角色和最低特权访问的原则应用于环境中所有的服务器。只有被授权具有特定权限的用户才能够获取服务器和区域内访问、读取、写入或执行的权限。

数据库服务器位于双重防火墙后以保护用户数据的安全，MTS采用了复杂的 反欺诈检测算法来即可识别和锁定访问。此外，客户服务历史记录数据使用 AES 256 位静态加密。

网络安全

MTS SmartService采用了业内最高等级的安全防护措施保护客户服务历史数据安全，提升用户体验。MTS SmartService的构架包括可靠的防火墙，可控的即时网络通讯监控，安全防护系统保护数据不被非授权获取。为了进一步提升数据安全，负载平衡的入侵检测系统(IDS)时刻分析所有网络通信，监控网络攻击和异常，提醒相关工程技术人员采取应对措施。由于网络攻击的方法也在不断发展和变化，因此需要在 IDS 模块上定期更新签名，以便检测和预防新的安全威胁。

亚马逊网络服务(AWS)的安全监控工具帮助识别拒绝服务(DoS)攻击，包括分布式攻击、同步洪流以及软件逻辑攻击等等。当DoS攻击被识别时，AWS服务将立即启动应对预案。除了DoS防护攻击工具，在不同地区和国家选择可靠的通信服务供应商也可以有效提升防止DoS攻击的能力。数据服务器经过强化并且关闭了不必要的服务，持续进行主动维护，以确保及时应用所有适当的安全修补程序。

物理层安全

» 所有区域均被实时监控，24x7x365的视频监控与警报系统；

» 亚马逊数据中心具有物理隔离，仅有被授权的AWS管理者才可以访问；

» 通过生物识别双重认证，只有授权人员才可访问服务器

供电与环境

» 可靠的持续供电与后备发电系统；

» 多重分布式供电系统保证最佳备份供电；

» 环境空调系统保持N+2 冗余配置；

» 可控通风、温度与湿度

防火与救灾

» 多区域喷淋灭火系统；

» 早期烟雾探测警报(VESDA)系统实时气体采样提供早期警报；

» 灭火系统水压双重监控

洪水与地震保护

» 所有设备放置于高于海平面的地区并且具有良好的水汽隔离，没有任何地下室；

» 湿度检测系统以及后备泵房用于排水；

» 所有设备厂房均超过当地的地震防护要求；

其他的特性

» 由多个供应商提供强大的网络连接；

» 配置了基于会话的故障转移的冗余防火墙；

» 冗余负载平衡以及核心光纤交换设备；

» 负载平衡入侵检测系统(IDS)

安全构架 – 保持可靠与可扩展的服务

MTS SmartService安全构架能够保持系统的持续工作以及可扩展能力。负载平衡自动跨区域分配传入的备份流量，并扩展请求处理容量以满足流量扩展的需求。

MTS SmartService使用至少两个工作区间，每个工作区间具有独立的物理构架，工程设计保证了系统极高的可靠性。一般常出现故障的设备，例如电力系统或者冷却系统，不会被各个工作区共享。某些关键点被物理隔离，也可以避免出现某些极端的灾害发生，例如火灾、飓风、洪水或者地震等等。MTS SmartService的物理构架保证了任何区域内出现问题不会影响整体的服务，也可以适应大数据的冲击而不影响性能。

物理层与网络

MTS SmartService使用了现在最先进的网络安全技术，其服务器托管在具有最高安全等级的超3 层数据中心设施之内。

MTS系统公司使用AWS服务，该服务分布于不同的地区以及时区内，AWS服务具有强壮的构架，所有服务由亚马逊网络服务以及构架专家提供。如果需要了解AWS的详细信息，请访问：http://aws.amazon.com/security/ 和http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf.

业务连续性以及灾后恢复

MTS SmartService服务器托管在具有最高安全等级的 超3 层数据中心，能够抵抗例如火灾、洪水或者地震等意外，其多层次的安全设置，分布式冗余的供电系统，环境控制系统等等保持服务器的持续工作。尽管具有高可用性功能，一旦数据中心出现意外不再可操作，AWS 仍可在多个地理位置独立的区域维护虚拟服务器基础设施，以便进行灾后恢复。AWS 拥有配置相同的故障转移数据中心，每个数据中心都具有冗余的容量和备用硬件，能够为客户提供灾后恢复。从备份数据中心恢复数据的时间不会超过24小时。

MTS SMARTSERVICE变更设备管理

MTS SmartService 采用严格的变更管理程序，提供与 ISO9001：2008 认证一致的方式处理变更规划、实施和跟进的全面方法。这种方法有效提高了客户服务的质量，其核心就是所有软件的变更均经过充分的审核、测试和跟踪，任何可能被影响的用户都会被及时通知知晓类似的变化对用户的影响。

在进行软件变更的时候，首先将变更需求通过书面形式提供给客户。变更需求被提交之后，相应的团队将审核需求，达成共识之后才进行下一步。在最后软件部署之前，所有的软件均被充分测试，例如通过 α 、β 测试之后的软件才会被正式部署。

MTS SMARTSERVICE监控与支持

MTS SmartService全年被实时监控，并且提供支持。集成化的系统、网络与传输监控工具监测不同层级的性能和可靠性矩阵，例如CPU的占有率、磁盘空间与可靠性等等。相应的警报信息能够被及时识别并且解决相应的问题。MTS的客户支持团队为客户提供全方位、及时的技术支持与服务。

美特斯工业系统(中国)有限公司
MTS Systems(China) Co., Ltd.

上海
电话：021–24151000
传真：021–24151199

北京
电话：010–65876888
传真：010–65876777

电邮：MTSC–Info@mts.com
http://www.mts.com

ISO 9001 Certified QMS

100–567–767 SmartServiceSecurity_ZH 4/20