《金融科技创新应用声明书》

创新应用基本信息	创新应用编号	91310000MA1FL0HA77-2020-0001	
	创新应用名称	“融通保”中小微企业票据流转支持产品	
	创新应用类型	科技产品	
	机构信息 1	统一社会信用代码	91310000MA1FL0HA77
		全球法人识别编码	300300M61YN8TL1KDU63
		机构名称	兴业数字金融服务(上海)股份有限公司
		持有金融牌照信息	无
	机构信息 2	统一社会信用代码	91350000158142711F
		全球法人识别编码	300300C1030935001303
		机构名称	兴业银行股份有限公司
		持有金融牌照信息	牌照名称:中华人民共和国金融许可证 机构编码:B0013H135010001 发证机关:中国银行业监督管理委员会
	拟正式运营时间	2020 年 07 月 01 日	
	技术应用	1.通过分布式账本技术，将产业链上下游数据信息加密上链，实现对多种参与主体线上交易的准确识别和追溯；利用存证机构的分布式节点，实现对操作流、信息流的分布式存储和使用。 2.基于云计算技术构建软件即服务(SaaS)服务平台，为金融机构的供应链金融服务提供支撑，支持其向各类实体企业输出集成化、标准化的金融服务。 3.运用大数据技术，建立反欺诈、反洗钱的模型，实现对票据流转业务的全流程监控，进一步提升金融机构风控水平。 4.基于人工智能技术，使用自动化机器人(RPA)代替人工进行后台运营操作，实现异常交易风险核查的自动化、智能化，提升运营效率。	
	功能服务	本产品运用分布式账本、人工智能、大数据、云计算等技术构建企业级 SaaS 服务平台。以平台为支撑，在保障数据安全的前提下，实现票据流、资金流、订单流的多流合一，以及核心数据的分布式存储，为企业与金融机构间的票据转让和贴现提供信息支撑服务，将传统模式下需要客户到线下网点办理的票据融资服务拓展到线上进行，同时实现业务申请的智能审核、自动放款以及在线秒贴，有效解决中小微企业持有票据贴现难、贴现慢的问题。 本项目由兴业数字金融服务(上海)股份有限公司和兴业银行	

		股份有限公司联合进行研发与运维，没有其他第三方参与，兴业数金公司负责技术开发与运维，兴业银行提供金融应用场景。
	创新性说明	1.基于产业链上下游数据的票据流、资金流、订单流多流合一，辅助票据转让、贴现服务的线上审核，提升业务自动放款的安全性。 2.通过 SaaS 服务平台将银行服务能力赋能至产业端，帮助银行向各类实体企业批量化输出金融服务。 3.基于嵌入式供应链金融服务模块，围绕供应链中关键企业为链属中小微企业提供服务，从源头控制票源真实性，实现对供应链上企业的精准服务。 4.通过在后台运营流程中应用智能机器人，提升业务及风险事件处理效率。 5.利用区块链技术可追溯、不可篡改的特点，实现对多种参与主体线上交易的准确识别和追溯，在满足信息校验需求的同时，更好的保障数据安全。
	预期效果	1.本项目通过对供应链链属企业数据进行交叉验证，提高了票据流转效率，将银票贴现业务从 2 个工作日缩短至 3 分钟内放款。 2.企业级平台的搭建，推进业务线上线下融合，优化金融服务流程，提升融资效率，帮助供应链链属企业、金融机构降本增效，为中小微企业持有的难以贴现融资的票据实现在线融通，助力企业疫后复工复产。
	预期规模	按照风险可控原则合理确定用户范围和服务规模。预计上线后年服务企业 1000 家，年流转票据 2 万笔，年流转规模 200 亿。
创新应用服务信息	服务渠道	1.通过 SaaS 平台向金融机构端提供服务。 2.基于嵌入式供应链金融服务模块，通过供应链中关键企业的互联网服务平台为其链属企业提供服务。
	服务时间	法定工作日 9:00-17:00
	服务用户	供应链属中小微企业
	服务协议书	《服务协议书-“融通保”中小微企业票据流转支持产品》（见附件 1-1）
合法合规性评估	评估机构	北京市金杜律师事务所上海分所
	评估时间	2020 年 06 月 28 日
	有效期限	1 年

	评估结论			本项目符合《中华人民共和国票据法》、《支付结算办法》（银发〔1997〕393号印发）、《中国人民银行金融消费者权益保护实施办法》（中国人民银行令〔2020〕第5号发布）等相关现行金融行业法律法规文件要求，不存在侵害客户数据安全和个人信息等违法情况。经评估，本项目符合金融科技创新监管试点合法合规性要求，可以依法合规开展业务。
	评估材料			《合法合规性评估报告-“融通保”中小微企业票据流转支持产品》（见附件1-2）
技术安全性评估	评估机构			中国金融电子化公司
	评估时间			2020年09月01日
	有效期限			1年
	评估结论			本项目严格按照《个人金融信息保护技术规范》（JR/T 0171—2020）、《网上银行系统信息安全通用规范》（JR/T0068—2020）、《区块链技术金融应用评估规则》（JR/T 0193—2020）、《金融科技创新安全通用规范》等相关金融行业技术标准规范要求进行设计开发并进行全面安全评估。经评估，本项目满足相关现行标准法规要求，符合在票据融通等金融场景中应用的条件。
	评估材料			《技术安全性评估报告-“融通保”中小微企业票据流转支持产品》（见附件1-3）
风险防控	风控措施	1	风险点	基于分布式账本技术的多主体多流（订单流、资金流、票据流）信息数据的分布式存储模式在金融领域尚无成熟经验可循，可能有潜在的安全风险，需要在试点环境中进行测试与验证。
			防范措施	对于分布式账本技术应用可能出现的风险。一是运用创新技术手段，采用多方数据进行交叉验证并结合分布式账本的技术特性，解决数据真实性等问题，系统直连银行信息系统，发布的信息均可通过银行信息系统查验真伪，从机制和技术上有效防范平台信息系统黑箱问题。二是业务风险管理方面，合规风控团队通过客户分层管理、限额监控等风控合规手段，预防和检测承兑风险。平台设置企业异常行为监测模块，每月对上月数据进行回溯，基于客户的当月及历史的交易行为数据判别其申请票据融通的合理性，对风险客户进行平台账号限制，防范违规套利等行为。三是内控合规管理方面，构建多层次、全方位、一体化的内部控制体系，有效防止内部人员的违规操作、内部欺

				诈与犯罪行为。
		2	风险点	云服务器在数据传输过程中如遇系统故障或运营管理不当，可能存在数据泄露或被篡改的安全风险。
			防范措施	针对数据泄露及相关风险，本项目在数据采集时，严格遵循“用户授权、最小够用、全程防护”原则，充分评估潜在风险，加强数据全生命周期安全管理，严防用户数据的泄露、篡改和滥用风险。数据采集时，将通过隐私政策文件等方式明示用户数据采集和使用目的，获得用户授权条件下方可采集；数据存储时，通过加密技术将原始数据脱敏，切实保护客户隐私，防止信息被窃取、篡改、破坏等恶意行为发生；数据使用时，严控数据访问权限，保障客户数据在授权范围内使用。数据传输时，采用传输通道加密等方式对数据进行加密、双向认证传输，在不归集、不共享原始数据前提下，仅向外提供脱敏后的计算结果，有效保障数据全生命周期安全。
		3	风险点	创新应用上线运行后，可能面临网络攻击、业务连续性中断等方面风险，亟需采取措施加强风险监控预警与处置。
			防范措施	在项目实施过程中，将按照《金融科技创新风险监控规范》建立健全风险防控机制，掌握创新应用风险态势，保障业务安全稳定运行，保护金融消费者合法权益。
	风险补偿机制	本项目按照由申请各方联合建立的风险补偿方案建立健全风险补偿机制（见附件 1-4），明确风险责任认定方式、制定风险赔付机制，配套风险拨备资金、保险计划等补偿措施，切实保障金融消费者合法权益。对于非客户自身责任导致的资金损失，提供全额补偿，充分保障消费者合法权益。		
	退出机制	本项目按照由申请各方联合建立的退出机制（见附件 1-5），在保障用户资金和信息安全的前提下，进行平稳退出。 在业务方面，按照退出方案终止有关服务，及时告知客户并与客户解除协议。如遇法律纠纷，按照服务协议约定进行仲裁、诉讼。涉及资金的，按照服务协议约定退还客户，对客户造成资金损失的通过风险补偿机制进行赔偿。 在技术方面，对系统进行下线。涉及数据的，按照国家及金融行业相关规范要求做好数据清理、隐私保护等工作。		

	应急预案	本项目按照由申请各方联合建立的应急预案(见附件 1-6)妥善处理突发安全事件，切实保障业务稳定运行和用户合法权益。在系统上线前进行全链路压测、容灾演练，对相关操作人员进行应急处置培训；在系统上线后定期开展突发事件处置演练，确保应急预案的全面性、合理性和可操作性。建立日常生产运行监控机制，7×24 小时实时监控系统运行状况，第一时间对核心链路、接口、功能模块、硬件资源等的异常情况进行告警。一旦发生突发事件，根据其影响范围和危害程度，及时采取有针对性措施进行分级分类处理，视需要及时关闭增量业务，妥善处置受影响的存量业务，切实保障用户资金和信息安全。	
投诉响应机制	机构投诉	投诉渠道	1.受理机构：兴业银行股份有限公司 2.投诉电话：95561 转 8 3.客户投诉受理邮箱:95561@cib.com.cn
		投诉受理与处理机制	项目组将秉持客观、公正、及时的原则，在接到投诉事件后，负责对事件进行了解和分析，在确认投拆原因和相关问题后，协调相关技术部门或业务部门进行处理解决，并及时将处理进度反馈投诉人员，全力解决相关问题。
	自律投诉	投诉渠道	受理单位：中国支付清算协会 投诉网站：http://cfp.pcac.org.cn/ 投诉电话：010-66001918 投诉邮箱：fintechts@pcac.org.cn
		投诉受理与处理机制	中国支付清算协会是经国务院同意、民政部批准成立的全国性非营利社会团体法人。为保护金融消费者合法权益，营造遵守国家宪法、法律、法规和社会道德风尚的良好金融科技创新监管试点环境，推动金融科技行业健康可持续发展，按金融管理部门工作要求，协会以调解的形式，独立公正地受理、调查以及处理金融科技创新监管试点中出现的投诉举报等相关事宜。 对于涉及相关试点城市的金融科技创新应用项目的投诉举报事项，中国支付清算协会将依照规定的程序进行调解，由协会举报中心对投诉情况进行沟通、记录后，

			相关业务部门负责进行调查处理。 联系方式：010-66001918 对外办公时间：周一至周五 上午 8:30-11:30，下午 13:30-17:00
备注	无		
承诺声明	我机构承诺所提交的材料真实有效，严格遵守相关金融管理要求，已全面开展合规性评估和内控审计，能够有效保障业务连续性和用户信息安全，防范资金失窃风险。本声明书正文与附件表述不一致的，以正文为准。 我机构承诺本产品符合《金融科技创新安全通用规范》。 以上承诺如有违反，愿承担相应责任与后果。 法定代表人或其授权人（签字） 2022年10月9日（盖章）		

“融通保”中小微企业票据流转支持产品用户注册服务协议

*该用户注册服务协议仅供相应业务参考

“融通保”中小微企业票据流转支持产品是整合了多终端售票工具、批量投资工具、投资后分析工具、及“执剑人”、“倚天鉴”两大工具的互联网票据信息平台。

在本平台进行注册并接受本协议约束的，即为本平台注册用户（以下简称“用户”），包括非认证用户和认证用户。非认证用户是指在本平台以用户名及密码进行注册，可以登录本平台，但未完成全部注册程序（包括企业认证、业务授权、账户绑定、创建执剑人账户等）的用户，非认证用户可以是自然人、法人或其他组织；非认证用户仅享有本平台提供的部分服务。认证用户是指在本平台完成注册并完成企业认证、业务授权、账户绑定、创建执剑人账户等注册程序的用户，认证用户必须是依据中华人民共和国法律在境内（不含香港、澳门特别行政区和台湾地区）设立的具有完全民事权利和民事行为能力，能够独立承担民事责任的法人和其他组织；认证用户享有本平台提供的全部服务。非认证用户在补充完成企业认证、业务授权、账户绑定、创建执剑人账户等注册程序后，则成为认证用户，并以认证用户的名义接受本协议的约束。

本平台（下称“平台”）、执剑人系统及倚天鉴系统的开发运营方兴业数字金融服务（上海）股份有限公司（以下简称“兴业数金公司”），隶属于兴业银行集团，通过为平台提供嵌入服务，利用科技手段为本平台用户提供在线开户、资金存管与监管、票据信息的真实性与有效性验证、票据流转状态进行判别等服务。**用户通过网络页面点击确认或以其他方式选择接受本协议并进行注册时，即表示用户与本平台已达成协议并同意接受本协议的全部约定内容、本平台与兴业数金公司等外部系统签署的相关协议、与本协议有关的各项规则以及本平台所包含的其他与本协议或本协议项下各项规则有关的各项规定、提示、告示、公示。 如果用户不同意本协议的任一内容，或者无法准确理解本平台对条款的解释，请不要进行后续操作。**

一、用户保证及承诺

1、用户必须依本平台、兴业数金公司要求提供真实、最新、有效及完整的资料，并且授予本平台、兴业数金公司基于提升提供相应综合性金融服务和网站服务的目的对其提供的资料及数据信息拥有永久的、免费的使用权利。

2、用户有义务维持并更新注册的用户资料，确保其为真实、最新、有效及完整。若用户提供任何错误、虚假、过时或不完整的资料，或者本平台、兴业数金公司依其独立判断怀疑资料为错误、虚假、过时或不完整，本平台有权暂停或终止用户在本平台的注册账号，并拒绝用户使用本平台服务的部分或全部功能。在此情况下，本平台、兴业数金公司不承担任何责任，用户同意承担因此所产生的直接或间接的任何支出或损失。

3、用户保证并承诺通过本平台依法合规进行票据的相应流转，相应的资金来源合法。

4、用户承诺，其通过本平台发布的信息均真实有效，其向本平台、兴业数金公司提交的任何资料均真实、有效、完整、准确。如因违背上述承诺，造成本平台或兴业数金公司方损失的，用户将承担相应责任。

5、用户同意，本平台有权在提供网站服务过程中以各种方式投放各种商业性广告或其他任何类型的商业信息，并且用户同意接受本平台通过电子邮件、手机短信或其他方式向用户发送商业信息。

6、用户承诺，放弃票据资金专户内资金利息的任何权利。

7、用户不得私自仿制、伪造在网站上签订的电子合同或印章，不得用伪造的合同进行招摇撞骗或进行其他非法使用，否则由用户自行承担责任。

二、网站服务

1、本平台服务内容主要包括票据流转信息发布和相关综合性服务。兴业数金公司通过“执剑人”系统为平台系统提供相应服务，利用科技手段为本平台用户提供在线开户、资金存管与监管、票据信息的真实性与有效性进行验证、对票据流转状态进行判别等服务。流转各方的流转内容和风险应由各方自行承担。

2、本平台通过网站为用户提供本合同约定的服务，该服务及平台系统由兴业数金公司运营管理。

3、本平台对于用户的通知及任何其他的协议、告示，**用户同意本平台通过网站公告、电子邮件、手机短信、站内通知等电子方式或常规的信件传递等方式进行，该等通知于发送之日视为已送达收件人。因信息传输等原因导致用户未在前述通知发出当日收到该等通知的，本平台不承担责任。**

4、在本平台流转需订立的合同采用电子合同方式。**用户使用注册用户名登录本平台后，根据本平台的相关规则或有关合同约定，在网站通过点击确认或约定方式签订的电子合同，即视为用户真实意思表示并以用户名义签订的合同，具有法律效力。**用户应妥善保管自己的注册用户名和密码等注册信息，用户通过前述方式订立的电子合同对合同各方具有法律约束力，用户不得以其注册用户名和密码等注册信息被盗用或其他理由否认已订立的合同的效力或不按照该等合同履行相关义务。

5、**用户根据本协议、网站的相关规则或有关合同约定签订电子合同后，不得擅自修改该合同。本平台向用户提供电子合同的备案、查看服务。如对此有任何争议，应以本平台记录的合同为准。**

6、**在不违反适用法律的强制性规定的前提下，本平台提供的服务有可能会发生变更或者增加。一旦本服务协议的内容发生变动，本平台将通过网站公布最新的服务协议，不再向用户作个别通知。如用户不同意本平台对本服务协议所做的修改，用户有权停止使用本平台服务。如果用户继续使用本平台服务，即表示同意接受经修订的协议和规则。如新旧规则或协议之间冲突或矛盾的，除另行明确声明外，以最新修订的协议和规则为准。**

三、风险提示

1、**用户知晓并同意，任何通过本平台进行的票据流转并不能避免以下风险的产生，本平台不能也没有义务为如下风险负责：**

（1）平台用户提供的信息和资料的真实性、完整性、有效性、合法性存在瑕疵；平台用户开展的与票据流转相关交易的合法性、合规性、有效性存在瑕疵；平台用户资金来源的合法性存在瑕疵； 平台用户使用未经兴业数金公司审核或认可的平台交易规则；票据流转交易项下票据非因兴业数金公司原因被采取冻结等限制措施影响平台用户票据权利行使或实现的；其他因平台用户的过错导致任何损

失或责任的情形。

（2）政策风险：有关法律、法规及相关政策、规则发生变化，可能引起相关等方面异常情况，用户有可能遭受损失。

（3）不可抗力因素导致的风险。

（4）因用户的过错导致的任何损失，该过错包括但不限于：决策失误、操作不当、遗忘或泄露密码、密码被他人破解、用户使用的计算机系统被第三方侵入、用户委托他人代理流转时他人恶意或不当操作而造成的损失。

（5）基于互联网的特殊性，兴业数金公司不担保系统不会中断，也不担保系统的及时性和/或安全性。因下列原因导致系统无法正常运作，甲方应当事先通知乙方，不能事先通知的，应当在发生后及时通知乙方，并采取补救措施，但不因此承担违约责任：平台系统停机维护期间;电信设备出现故障不能进行数据传输的;由于黑客攻击、网络供应商技术调整或故障、网站升级、银行方面的问题等原因而造成的平台服务中断或延迟。

2、本平台不对任何用户及/或任何流转提供任何明示或默示的担保。本平台向用户提供的各种信息及资料仅为参考，用户应依其独立判断做出决策。用户据此进行票据流转的，产生的风险由用户自行承担，用户无权据此向本平台提出任何法律主张。在票据流转过程中，各方发生的纠纷，平台将协助解决，但平台不承担任何责任。

3、以上并不能揭示用户通过本平台进行票据流转的全部风险及市场的全部情形。用户在做出决策前，应全面了解相关流转规则，谨慎决策，并自行承担全部风险。

四、服务费用

当用户使用本平台服务时，本平台会向部分用户收取相关服务费用。各项服务费用以平台相关公告为准。具体收费亦可联系平台运营团队详询。本平台保留单方面制定及调整服务费用的权利。

五、用户安全及管理

1、**用户知晓并同意，确保用户注册用户名及密码的机密安全是用户的责任。用户将对利用该注册用户名及密码所进行的一切行动及言论，负完全的责任，并同**

意以下事项：

（1）用户不对其他任何人泄露注册用户名或密码，亦不可使用其他任何人的本平台注册用户名或密码。因黑客、病毒或用户的保管疏忽等非本平台原因导致用户的注册用户名遭他人非法使用的，本平台不承担任何责任。

（2）本平台、兴业数金公司通过用户的注册用户名及密码来识别用户的指令，用户确认，使用用户注册用户名和密码登录后在本平台的一切行为均代表用户同意。用户注册用户名操作所产生的电子信息记录均为用户行为的有效凭据，并由用户承担由此产生的全部责任。

（3）冒用他人注册用户名及密码的，本平台及其合法授权主体保留追究实际使用人连带责任的权利。

2、**用户如发现有第三人冒用或盗用用户注册用户名及密码，或其他任何未经合法授权的情形，应立即以有效方式通知本平台，要求本平台暂停相关服务，否则由此产生的一切责任由用户单位承担。同时，用户理解本平台对用户的请求采取行动需要合理期限，在此之前，本平台对第三人使用该服务所导致的损失不承担任何责任。**

3、**用户决定不再使用注册用户名时，并向本平台申请注销该注册用户名。注册用户名被注销后，用户与本平台基于本协议的合同关系终止，本平台没有义务为用户保留或向用户披露注册用户中的任何信息，但本平台仍有权继续使用该用户在接受网站服务期间发布的所有信息。**

六、用户的守法义务

1、**用户承诺绝不为任何非法目的或以任何非法方式使用本平台服务，并承诺遵守中华人民共和国相关法律、法规及一切使用互联网之行业惯例、国际惯例，遵守所有与本平台服务有关的网络协议、规则。**

2、在接受本平台服务的过程中，用户承诺不从事下列行为：

（1）发表、传送、传播、储存侵害他人知识产权、商业秘密权等合法权利的内容。

（2）制造虚假身份、发布虚假信息等误导、欺骗他人，或违背本平台页面公布之规则、提示、公示、公告进行虚假流转。

（3）进行危害计算机网络安全的行为。

3、在使用本平台服务的过程中，用户承诺遵守以下约定：

（1）在使用本平台服务过程中实施的所有行为均遵守国家法律、法规及本平台各项规则，不违背社会公共利益或公共道德，不损害他人的合法权益。

（2）不发布国家禁止发布的信息，不发布其它涉嫌违法或违反本协议及各类规则的信息。

（3）不对本平台上的任何数据作商业性利用，包括但不限于在未经本平台事先书面同意的情况下，以复制、传播等任何方式使用本平台上展示的资料。

4、用户了解并同意：

（1）违反上述承诺时，本平台有权依据本协议的约定，做出相应处理或终止向用户提供服务，且无须征得用户的同意或提前通知该用户。

（2）当用户的行为涉嫌违反法律法规或违反本协议和/或规则的，本平台有权采取相应措施，包括但不限于直接屏蔽、删除侵权信息，或直接停止提供服务。如使本平台遭受任何损失的（包括但不限于受到第三方的索赔、受到行政管理部门的处罚等），用户还应当赔偿或补偿本平台遭受的损失及（或）发生的费用，包括诉讼费、律师费、保全费等。

5、用户同意，由于违反本协议，或违反其在平台上签订的协议或文件，或由于用户使用本平台服务违反了任何法律或第三方的权利而导致任何第三方向本平台提出的任何补偿申或要求（包括律师费用），用户必须对本平台给予全额补偿并使之不受损害。

七、隐私条款

1、本平台对于用户提供的、本平台自行收集的、经认证的身份信息将按照本协议予以保护、使用或者披露。未经本平台事先书面同意，用户不得转让其在本协议项下的任何权利和义务。

2、为了提升综合性金融服务体验，用户同意授权本平台及其代理机构、建立业务合作关系的机构等，以便核对用户的注册信息等。

3、为提升相应的综合性服务质量，本平台将按照用户在平台上的行为自动追踪关于用户的某些资料。用户同意本平台有权对整个用户数据库进行分析并对用

户数据库进行必要的使用。

4、用户同意本平台可使用用户的相关资料（包括但不限于本平台持有的用户档案中的资料，本平台从用户目前及以前在本平台平台上的活动所获取的其他资料，以及本平台通过其他方式自行收集的资料）以解决争议、对纠纷进行调停。用户同意本平台可通过人工或自动程序对用户资料进行评价。

5、本平台、兴业数金公司采用行业标准惯例以保护用户的资料。用户因履行本协议提供给本平台的信息，本平台、兴业数金公司不会恶意出售或共享给任何第三方，以下情况除外：

（1）提供独立服务且仅要求服务相关的必要信息的供应商，如印刷厂、邮递公司等。

（2）具有合法调阅信息权限并从合法渠道调阅信息的政府部门或其他机构，如公安机关、法院。

（3）本平台的关联方。

（4）协调处理与平台上用户之间流转相关的争议。

6、 本平台有义务根据有关法律要求向司法机关和政府部门提供用户的资料。在用户未能按照与本平台签订的服务协议或者与网站其他用户签订的协议等法律文本的约定履行自己应尽的义务时，本平台有权根据自己的判断，或者与该笔流转有关的其他用户的请求披露用户的信息资料，并做出评论。用户严重违反本平台相关规则的，本平台有权对用户提供的及本平台自行收集的用户信息和资料编辑入网站黑名单，并将该黑名单对第三方披露，且本平台有权将用户提交或本平台自行收集的用户资料和信息与任何第三方进行数据共享，由此可能造成的用户的任何损失，本平台不承担法律责任。

7、 本平台使用 Cookie 来帮助用户实现联机体验的个性化。Cookie 是由网页服务器存放在用户硬盘中的文本文件。Cookie 不能用来运行程序或将病毒递送到 用户的计算机中。指定给用户的 Cookie 是唯一的，它只能由将 Cookie 发布给 用户的域中的 Web 服务器读取， Cookie 会帮助本平台在用户后续访问时调用用户的特定信息。这样可以简化记录用户信息，当用户下次使用本平台服务时，系统会自动调出用户以前发布或浏览的信息，使用户的使用变得更加便捷和高效。

八、知识产权声明

本平台拥有网站内所有信息内容，包括但不限于文字、图片、软件、音频、视频等的版权。非经本平台书面同意，任何组织或个人都不得复制、打印和传播属于本平台的信息内容用于其他目的。网站所有的产品、技术及程序均属于本平台知识产权，未经本平台许可，任何人不得擅自使用（包括但不限于以非法的方式复制、传播、展示、下载等）。否则，本平台将依法追究其法律责任。

九、条款的解释、法律适用及争端解决

1、本协议是由用户与本平台签订的，适用于用户在本平台的全部活动。本协议内容包括但不限于协议正文条款及已经发布的或将来可能发布的各类规则、本平台网页上的各类提示、告示、公告，所有条款和规则、提示、告示、公告为协议不可分割的一部分，与协议正文具有同等法律效力。

2、本协议不涉及用户与本平台的其他用户之间，因网上流转而产生的法律关系及法律纠纷，但用户在此同意将全面接受并履行与本平台其他用户在平台签订的任何电子法律文本，并承诺按照该法律文本享有和（或）放弃相应的权利、承担和（或）豁免相应的义务。

3、因本协议之效力、解释、变更、执行与争议解决均适用中华人民共和国法律。如无相关法律规定，可参照商业惯例和（或）行业习惯。

4、因本协议产生的争议，应当协商解决，协商不成提交上海仲裁委员会解决。

本协议最后更新版本：2019 年 06 月 24 日

金杜律师事务所
KING&WOOD
MALLESONS

上海市淮海中路999号
上海环贸广场写字楼一期16-18层 邮编200031

16-18/F, One ICC, Shanghai ICC
999 Huai Hai Road, Shanghai, 200031, China

T +86 21 2412 6000
F +86 21 2412 6150

www.kwm.com

备忘录

严格保密

日 期 二〇二〇年六月二十八日

收件人 兴业数字金融服务(上海)股份有限公司("兴业数金"或"贵司")

发件人 北京市金杜律师事务所上海分所("本所"或"我们")

事 由 关于"融通保"中小微企业票据流转支持平台产品的法律分析

敬启者:

我们谨提及近期关于题述事项的讨论。我们理解,贵司已设立、运营和管理的"融通保"平台("**平台**")在日常经营业务过程中为商业银行和企业等法人主体提供商业承兑汇票或银行承兑汇票("**票据**")信息撮合、票据交易见证和资金代管等票据流转相关服务。为进一步落实《金融科技(FinTech)发展规划(2019-2021 年)》的要求,贵司拟将本项目向中国人民银行营业管理部申请作为上海地区金融科技创新监管试点应用项目("**新背景**")。根据与贵司的沟通,贵司在该等新背景下对本项目的技术创新应用说明、应用功能、预期效果进行了进一步的归纳,基于此,我们将在本备忘录中对本项目自身的合法性与合规性进行分析、归纳和提示,同时就本项目在新背景下继续适用该等模式的可行性作相应探讨。

一、 票据交易的合法合规性关注点

基于平台交易安排,我们理解,用户之间通过平台主要开展以票据为标的资产的交易。在我国,票据的流转、交易和相关活动应当受《票据法》的规范。同时,票据作为一种传统且常见的支付结算工具,其应当受中国人民银行颁布和实施的《支付结算办法》及其他票据业务相关的法规、部门规章和规范性文件的约束。目前,票据流转产品根据票据业务相关主体分属于银行业金融机构或普通企业法人主体大致可进一步分为企业与企业之间、企业与银行之间以及银行与银行之间各自进行的票据流转活动。

1. 转让方为企业,受让方为银行

根据《中国人民银行关于印发<商业汇票承兑、贴现与再贴现管理暂行办法>的通知》(银发[1997]216 号,"**216 号文**")的规定,贴现系指商业汇票的持票人在汇票到期日前,为了取得资金贴付一定利息将票据权利转让给金融机构的票据行为,是金融机构向持票人融通资金的一种方式,贴现的商业汇票应以真实、合法的商品交易为基础。同时,根

据《支付结算办法》的规定，在银行开立存款账户的企业法人以及其他组织作为持票人，在其与出票人或者直接前手之间具有真实的商品交易关系并能够提供与其直接前手之间的增值税发票和商品发运单据复印件的，可以向银行办理贴现，贴现时应作成转让背书。

我们理解，在本产品项下，如转让方为企业，受让方为银行，双方之间达成的票据流转系为216号文规定的票据贴现行为，在转让方系为票据项下合法持票人的情形下，其可以与银行之间开展票据贴现业务活动。

2. 转让方与受让方均为银行

根据216号文的规定，转贴现系指金融机构为了取得资金，将未到期的已贴现商业汇票再以贴现方式向另一金融机构转让的票据行为，是金融机构间融通资金的一种方式，转贴现的票据应以真实、合法的商品交易为基础。同时，根据《支付结算办法》的规定，贴现银行可持未到期的票据向其他银行转贴现，转贴现亦应作成转让背书。

我们理解，在本产品项下，如转让方和受让方均为银行，双方之间达成的票据流转系为216号文规定的票据转贴现行为，在票据本身有真实合法的商品交易基础的情况下，银行之间开展票据转贴现业务活动。

就银行和企业之间开展贴现业务和银行与银行之间开展转贴现业务中贴现申请人是否仍然需要根据上述规定提交发票和单据等文件，根据《中国人民银行关于规范和促进电子商业汇票业务发展的通知》(银发[2016]224号，"**224号文**")的规定，企业申请电票贴现无需向金融机构提供合同、发票等资料。对此，我们理解，该等规定主要系基于电子商业汇票系统(ECDS)的应用以及票据在签发时开票银行已经对票据对应的交易基础进行了审验与核查等前提条件，并且224号文本身系为规范性文件，层级低于《票据法》和前述各部门规章，该等规定是否能够改变上述对于票据本身应当以真实合法的商品交易作为基础的要求需在实践中作进一步观察。

二、 平台产品资金移转和交付安排相关关注点

就本产品项下资金流相关安排，我们理解，其可能涉及贵司未取得支付业务许可证的情况下从事第三方支付业务，或被认定为直接或间接归集用户资金以及从事交易所业务等风险。我们就该等产品安排相关分析详见我们此前于2018年6月6日向贵司发送的《关于票据流转平台业务的法律分析》及2019年12月2日向贵司发送的《关于票据流转平台更新业务模式的法律分析》中相关内容，此处不再赘述。

三、 新背景下本项目相关关注点探讨

基于《金融科技(FinTech)发展规划(2019-2021年)》的要求，金融科技为促进普惠金融发展提供新机制，同时可为防范化解金融风险的新利器。结合我们从公开渠道了解到的信息，2019年末，中国人民银行会同发改委、科技部、工信部、人社部和卫健委等六

部门批准在北京、上海、江苏、浙江、福建、山东、广东、重庆、四川、陕西等 10 省(市)开展为期 1 年的金融科技应用试点。

从促进普惠金融发展的角度，本项目项下，平台为商业银行和企业等法人主体提供票据信息撮合、票据信息管理、票据交易见证和资金代管等票据流转相关服务，一方面，基于 SAAS 平台，通过应用程序接口(API)向金融机构端提供服务，另一方面，基于嵌入式供应链金融服务模块，通过核心企业官网为其链属企业提供服务。基于此，从本项目开展的最终结果来看，一方面，为金融机构降低服务门槛和成本，另一方面，为供应链上下游企业提供高效便捷的融资渠道，力求解决供应链资金配置失衡问题。

从防控风险的角度而言，根据贵司提供的《金融科技创新应用声明书》及根据贵司的沟通，贵司同时设置了建模过程排除敏感信息及遵循"用户授权、最小沟通、全程防护"的原则上加强数据存储技术保护用户信息安全的风险补偿机制。同时，平台运用区块链、人工智能及云计算等技术，积极配合实施穿透式监管，通过系统接口准确上送经营数据，有助于监管机构掌握市场动态，从监管层面把控市场风险，为后续其他监管措施落实提供基础。

基于上述平台提供服务及技术的运用，我们理解，在平台被纳入上海金融科技创新监管试点应用平台的情形下，鉴于人民银行同时为票据业务和资金支付业务等金融相关业务的监管部门，本产品现阶段系在一定程度上符合上述普惠金融的目的且在一定程度上助于监管机构防控风险，在后续监管机构将该项目作为金融创新应用公示，贵司积极配合监管机构要求报送数据，并根据监管机构要求稳步落实退出机制的基础上，在短期内平台产品合规性具有一定解释空间。

基于与贵司的沟通以及贵司的相应介绍，本产品项下相关金融科技服务旨在以相关法律法规精神为准绳，协助相关监管部门理顺供应链链属企业的票据流转通道，以确保依法合规开展业务，从而实现纾解中小微企业融资难与融资贵等问题。

免责声明

我们仅根据本法律备忘录出具日有效的中国现行法律、法规和规范性文件、主管部门监管口径和我们届时对市场实践的观察出具本法律备忘录。我们不就本法律备忘录所涉交易的任何税务问题，或因本法律备忘录所引致或可能引致的任何税务问题发表任何意见。我们并不保证该等中国法律、法规和规范性文件、主管部门监管口径和市场实践在本法律备忘录出具之日后所发生的任何变化或被作出的任何解释对本法律备忘录不会产生影响。本法律备忘录仅供贵司就题述事宜之目的而使用。未经我们事先许可，本法律备忘录不得为任何其他目的被第三方所依赖或者向第三方披露。

顺祝商祺！

北京市金杜律师事务所上海分所

二〇二〇年六月二十八日

报告编号：XYSJRTB-安全评估报告-20200921

兴业数字金融服务(上海)股份有限公司“融通保”中小微企业票据流转支持产品技术性安全评估报告

产品名称（版本号）	“融通保”中小微企业票据流转支持产品 V1.0.0
委托单位	兴业数字金融服务（上海）股份有限公司
测评单位	中国金融电子化公司测评中心
报告时间	2020-09-21

中国金融电子化公司测评中心

报告编号：XYSJRTB-安全评估报告-20200921

兴业数字金融服务(上海)股份有限公司“融通保”中小微企业票据流转支持产品技术性安全评估报告

委托单位	兴业数字金融服务（上海）股份有限公司
产品名称（版本号）	“融通保”中小微企业票据流转支持产品 V1.0.0
检测类别	委托检测
审核人	
批准人	
报告时间	2020-09-21

中国金融电子化公司测评中心

评 估 报 告 声 明

1. 评估报告经签字、盖章后有效。
2. 本评估报告仅适用于本报告明确指出的委托单位被测样品。
3. 未经本机构书面批准，不得复制本报告中的内容（全文复制除外），以免本报告的使用者对被测样品做出不全面的评价。
4. 在任何情况下，若需引用本报告中的结果或数据都应保持其本来的意义，不得擅自增加、修改、伪造或掩盖本报告的原有内容。
5. 本报告不得复制作为广告材料使用。
6. 当被测样品版本变更或其它任何改变时，本报告检测结果不再适用，涉及到的任何技术、模块或子系统、甚至整个系统都必须按监管机构的要求进行必要的备案或重新检测。不得将本报告检测结果应用于其他版本的被测样品。
7. 本报告的检测结果描述反映的是截至 2020 年 09 月 21 日的情况。由于这些内容在将来可能发生变化或不再适用，任何基于这些信息作出的判断和分析都有可能面临风险。
8. 本报告检测结果的有效性建立在委托单位提供相关信息的真实性基础之上。对于由于委托单位提供不实信息而导致检测结果出现错误的情况，本机构不予负责。
9. 如对本报告的检测结果有异议，请于收到评估报告后 15 日内与本机构联系。
10. 本机构根据特定技术标准出具检测结果为“符合”的检测项仅表明被测样品的业务项符合了相应标准的要求，并不保证该被测样品或者该项业务是绝对安全的。

联系单位：中国金融电子化公司

地　　址：北京市大兴区西红门镇中国人民银行软件开发中心

联 系 人：　郭大圣

Email　：guodasheng@icfcc.com

联系方式：18600870269

目 录

技术性安全评估结论

产品名称	“融通保”中小微企业票据流转支持产品
产品简介	“融通保”中小微企业票据流转支持产品运用分布式账本、云计算等技术构建企业级 SaaS 服务平台。以平台为支撑，在保障数据安全的前提下，实现票据流、资金流、订单流的多流合一，以及核心数据的分布式存储，为企业与金融机构间的票据转让和贴现提供信息支撑服务，将传统模式下需要客户到线下网点办理的票据融资服务拓展到线上进行，同时实现业务申请的智能审核、自动放款以及在线秒贴，有效解决中小微企业持有票据贴现难、贴现慢的问题。
评估过程简介	中国金融电子化公司测评中心于 2020 年 09 月 01 日至 2020 年 09 月 21 日对“融通保”中小微企业票据流转支持产品开展了技术性安全评估工作。评估的过程包括评估准备、方案编制、现场评估及分析与报告编制。评估的范围包括信息保护、交易安全、网络安全、业务连续性、区块链(基础版)、云计算和内控管理等七方面内容。
评估结论	**基本符合**

总体评价

中国金融电子化公司测评中心依据《金融科技创新安全通用规范(试行)》对兴业数字金融服务（上海）股份有限公司送检的“融通保”中小微企业票据流转支持产品进行技术性安全评估，总体情况如下：

信息保护方面，用户在融通保系统注册时，在页面显示《平台用户注册服务协议》、《执剑人使用协议》，获得用户明示同意后，方可开展有关个人金融信息的收集活动；融通保系统采用授权书模式向用户说明情况，并按照授权书范围合规使用，未收集与所提供服务无关的个人金融信息；对于用户的手机号、证件号、银行卡号、银行行号等信息，银行卡号进行了屏蔽展示，但手机号、证件号未进行屏蔽展示。

交易安全方面，票据买方、卖方签署协议上链成功后，若是线上交易的话，需买方进行线上交易，买方操作员输入手机号、登录密码、短信验证码登录到执剑人系统，选择相应的订单，输入支付密码后，该笔订单支付成功，对该笔交易进行了支付验证和确认；申请机构接入了 SMARTBI（应用层）、Pingpoint，对异常交易及行为进行监控，发现异常时，会对用户进行实时短信通知。

网络安全方面，融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业务），不涉及 APP，故仿冒检测项不适用；融通保系统通过在页面显示客户预留信息或通过 Host 校验和 Referrer 校验手段进行防钓鱼防范，并与 CNCERT 福建分中心建立互联网仿冒应用监测和处置的合作机制；申请机构对应用系统进行了渗透测试，并提供了渗透测试报告，确保应用系统的安全性。

业务连续性方面，申请机构机房采用市电双路，对 UPS 等重要设备进行了监控报警，该产品部署于兴业数金私有云上，云平台为分布式架构，具备高冗余、高抗故障风险能力；申请机构制定了《兴业数字金融服务（上海）股份有限公司业务连续性管理办法》、《兴业数字金融服务（上海）股份有限公司托管业务系统业务连续性计划》、《兴业数字金融服务（上海）股份有限公司业务连续性总体应急预案管理办法》、《兴业数字金融服务股份有限公司生产数据管理规定》、《兴业数金数据备份策略》等制度，业务连续性及备份与管理方面符合要求；但申请机构对于 DDoS、网络钓鱼等重要安全威胁，暂未开展有相关单位、部门参与的联合演练，暂未制定员工在业务连续性方面的培训计划和考核标准。

技术使用安全：区块链(基础版)方面,区块链使用的对称密码算法为 AES(业务数据加密),非对称密码算法为 ECDSA(数字签名、公钥加密和密钥交换)，哈希算法为 SHA256(摘要算法，生成 256bit 的摘要)，节点通信采用 tls 双向认证，保证了节点通信过程中的完整性和保密性，但区块链部署环境暂未进行等级保护的安全评估；云计算平台采用 openstack 技术使用 kvm 实现虚拟化，支持多虚拟机的管理与配置、支持计算资源池化，能够动态调整 CPU、内存资源等。

内控管理方面，申请机构制定了《融通保_金融科技创新应用内控管理制度》、《融通保系统应急预案》、《融通保风险补偿机制》、《兴业银行信息科技系统突发事件应急处置细则》、《兴业银行集团信息安全事件应急处置规程》等制度，对金融科技应用的必要性、可行性、战略规划、风险防范、运营策略、内部审计和外部评估等内容进行规范化管理。

本次技术性安全评估共检测 130 个检测项，判定结果为“符合”的有 98 项，判定结果为“部分符合”的有 6 项，判定结果为“不符合”的有 3 项，判定结果为“不适用”的有 23 项。从本次技术性安全评估的结果看，系统还存在一些可进一步完善的方面，现对委托方兴业数字金融服务（上海）股份有限公司送检的“融通保”中小微企业票据流转支持产品提出如下建议：

信息保护方面，建议应对用户的手机号、证件号进行屏蔽显示；网络安全方面，建议部署防网络钓鱼工具，并制定应用系统紧急补丁发布的流程方案；业务连续性方面，应定期对产品的业务连续性进行审计，对于 DDoS、网络钓鱼等重要安全威胁，定期开展有相关单位、部门参与的联合演练，应制定员工在业务连续性方面的培训计划和考核标准；区块链(基础版)方面，区块链部署的环境应进行等级保护安全评估，以确保部署环境的安全性。

兴业数字金融服务（上海）股份有限公司“融通保”中小微企业票据流转支持产品已具备了基本的安全保护措施，但在信息保护、网络安全、业务连续性、区块链方面仍存在一些问题。结合风险评价与风险对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的危害情况，兴业数字金融服务（上海）股份有限公司“融通保”中小微企业票据流转支持产品在本次技术性安全评估结果中存在不符合项及部分符合项，但不会导致本产品面临高等级的安全风险，因此对本产品的基本安全状态进行综合判断，得出技术性安全评估的结论为基本符合。

综合判定：兴业数字金融服务（上海）股份有限公司“融通保”中小微企业票据流转支持产品基本符合《金融科技创新安全通用规范(试行)》的要求。

1. 概述

1.1 检测目标

本次检测目标是在兴业数字金融服务（上海）股份有限公司“融通保”中小微企业票据流转支持产品版本确定的基础上，对“融通保”中小微企业票据流转支持产品的信息保护、交易安全、网络安全、业务连续性、区块链(基础版)、云计算、内控管理等七个方面内容进行安全检测，客观、公正评估“融通保”中小微企业票据流转支持产品技术标准符合性和安全性，保障“融通保”中小微企业票据流转支持产品的安全稳定运行。

1.2 检测依据和标准

《金融科技创新安全通用规范(试行)》

1.3 被测软件概述

“融通保”中小微企业票据流转支持产品运用分布式账本、云计算等技术构建企业级 SaaS 服务平台。以平台为支撑，在保障数据安全的前提下，实现票据流、资金流、订单流的多流合一，以及核心数据的分布式存储，为企业与金融机构间的票据转让和贴现提供信息支撑服务，将传统模式下需要客户到线下网点办理的票据融资服务拓展到线上进行，同时实现业务申请的智能审核、自动放款以及在线秒贴，有效解决中小微企业持有票据贴现难、贴现慢的问题。

2. 评估环境

2.1 硬件/软件环境

序号	IP 地址	设备用途	操作系统版本	中间件	物理位置
1	10.32.61.1	Nginx 负载均衡	Centos7.6	Nginx	上海市浦东新区宁桥路 999 号 8 号楼
2	10.32.61.3	Nginx 负载均衡	Centos7.6	Nginx	上海市浦东新区宁桥路 999 号 8 号楼

序号	IP 地址	设备用途	操作系统版本	中间件	物理位置
3	10.32.61.129	应用服务器	Centos7.6	Tomcat	上海市浦东新区宁桥路 999 号 8 号楼
4	10.32.61.130	应用服务器	Centos7.6	Tomcat	上海市浦东新区宁桥路 999 号 8 号楼
5	10.32.61.135	应用服务器	Centos7.6	Tomcat	上海市浦东新区宁桥路 999 号 8 号楼
6	10.32.61.134	应用服务器	Centos7.6	Tomcat	上海市浦东新区宁桥路 999 号 8 号楼
7	10.32.61.136	应用服务器	Centos7.6	Tomcat	上海市浦东新区宁桥路 999 号 8 号楼
8	10.32.61.131	应用服务器	Centos7.6	Tomcat	上海市浦东新区宁桥路 999 号 8 号楼
9	10.160.11.5	数据库服务器	Centos7.6	Mysql	上海市浦东新区宁桥路 999 号 8 号楼
10	10.160.11.6	数据库服务器	Centos7.6	Mysql	上海市浦东新区宁桥路 999 号 8 号楼
11	10.32.10.31	Fabric-peer	Rhel7.4	goleveldb	数金通联机房
12	10.32.10.32	Fabric-peer	Rhel7.4	goleveldb	数金通联机房
13	10.32.11.52	Fabric-peer	Rhel7.4	goleveldb	数金通联机房
14	10.32.11.53	Fabric-peer	Rhel7.4	goleveldb	数金通联机房
15	122.224.240.250	Fabric-peer	Rhel7.4	goleveldb	钱塘公证处机房
16	119.97.218.102	Fabric-peer	Rhel7.4	goleveldb	千麦司法鉴定中心机房
17	122.224.109.58	Fabric-peer	Rhel7.4	goleveldb	武汉江天公证处机房
18	121.28.134.162	Fabric-peer	Rhel7.4	goleveldb	河北燕赵公证处机房

2.2 检测工具

序号	检测工具名称及版本	检测工具应用说明
1	Tcpdump Verion4.9.2	日志抓包

序号	检测工具名称及版本	检测工具应用说明
2	Wireshark Version3.2.4	日志分析

3. 评估方法

本次现场检测工作采用访谈、检查、测试等方法。

其中访谈是检测人员通过与被测系统有关人员进行交流、讨论等活动以获取证据的一种方法；访谈使用到的工具主要是访谈列表。检测人员针对访谈列表上的问题，逐项与客户端软件有关人员进行交流、讨论，根据被访谈人员的回答了解和确认客户端软件的安全保护情况；

检查是检测人员通过对检测对象进行观察、查验、分析等活动以获取证据的一种方法；检查使用到的工具主要是核查列表。检测人员针对核查列表上的问题，通过观察、查验、分析等活动，逐项核实。根据检查对象的不同，检查可以进一步分为文档审查、现场观测和配置核查等方式；

测试可以细分为工具测试和手工验证等，类型包括功能测试、安全测试等。其中工具测试是指利用抓包同工具对目标设备进行通讯报文的抓取，并用日志分析工具进行分析，直观地验证系统平台的安全状况。包括信息获取、密码分析等方式。手工验证是指根据要求上机验证安全功能和配置的实现情况。

4. 评估内容及结果

4.1 信息保护

4.1.1 全生命周期防护

测评对象	测评指标	结果记录	结果判定	问题编号
收集	应采取技术措施（如弹窗、明显位置 URL 链接等），引导个人金融信息主体查阅隐私政策，并获得其明示同意后，开展有关个人金融信息的收集活动。	用户在融通保系统注册时，在页面有《平台用户注册服务协议》、《执剑人使用协议》，并获得其明示同意后，开展有关个人金融信息的收集活动。	符合	
	应遵循合法、正当、必要的原则，向个人金融信息主体	融通保系统采用授权书模式向用户说明情	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	明示收集与使用个人金融信息的目的、方式、范围和规则等，不得收集与所提供服务无关的个人金融信息。	况，并按照授权书范围合规使用，未收集与所提供服务无关的个人金融信息。		
	应通过受理终端、客户端应用软件、浏览器等方式收集C3（用户鉴别信息）类别个人金融信息时，应使用加密等技术措施保证数据的保密性，防止其被未授权的第三方获取。	融通保系统在传输过程中，通过 https 协议加密，防止其被未授权的第三方获取。	符合	
	客户端应用软件向移动终端操作系统申请权限时，应遵循最小权限原则。	融通保系统以应用系统方式向金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业 务），不涉及 APP,故此项不适用。	不适用	
	应确保收集个人金融信息来源的可追溯性。	客户从开始注册、签约、交易，都有唯一的 ID 保持全流程的一致性，所有的信息都会记录到数据库，以此对个人信息进行追溯。	符合	
	不应委托或授权无金融业相关资质的机构收集 C3（用户鉴别信息）、C2(可识别主体身份与金融状况的个人金融信息）类别个人金融信息。	申请机构通过融通保系统收集个人信息（非个人金融信息），为内部收集，未委托或授权其它机构收集个人信息，故此检测项不适用。	不适用	
传输	应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的安全传输，如安全通道、数据加密等技术措施。	融通保系统在传输过程中，通过 https 协议加密，保证个人信息的安全传输。	符合	
	个人金融信息传输的接收方应对接收的个人金融信息进行完整性校验。	融通保系统在传输过程中，通过 https 协议加密，并通过 SHA1WtihRSA 进行签	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		名，接收方收到后进行验签，保证了个人信息的完整性。		
存储	受理终端、个人终端及客户端应用软件均不应存储银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除。	客户通过融通保进行注册签约时，若是选择线上交易，签约鉴权的时候，会输入银行账户名称、银行账户卡号进行鉴权，但不会存储银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等支付敏感信息。	符合	
	不应留存非本机构的银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等 C3（用户鉴别信息）类别个人金融信息。若确有必要留存的，应取得个人金融信息主体及账户管理机构的授权。	客户通过融通保进行注册签约时，若是选择线上交易，签约鉴权的时候，会输入银行账户名称、银行账户卡号进行鉴权，但未留存非本机构的银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN 和 CVN2）、银行卡密码、网络支付密码等 C3（用户鉴别信息）类别个人金融信息。	符合	
	C3（用户鉴别信息）类别个人金融信息应采用加密措施确保数据存储的保密性。	融通保系统在用户注册签约时，会收集用户的手机号、证件号、银行卡号、银行行号、所属银行信息，但未留存 C3 类别个人金融信息，故此检测项不适用。	不适用	
	应将个人生物识别信息的样本数据、模板与银行账号或支付账号、身份证号等用户个人隐私信息进行隔离存	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
	储。	企业与企业间票据流转业 务），不涉及个人生物信息，故该检测项不适用。		
使用	对于银行卡号、手机号码、证件类识别标识或其他识别标识信息等可以直接或组合后确定个人金融信息主体的信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应进行用户身份验证，并做好此类信息管理，防范此类信息泄露风险。	融通保系统在用户注册签约时，会收集用户的手机号、证件号、银行卡号、银行行号、所属银行信息，展示时对银行卡号进行了屏蔽展示，但手机号、证件号、姓名未进行屏蔽展示。	部分符合	XYSJ-001
	后台系统应对支付账号、客户法定名称、支付预留手机号码、证件类或其他类识别标识信息等展示宜进行屏蔽处理，如需完整展示，应做好此类个人金融信息管理，采取有效措施防范未经授权的拷贝。	经查看数金后台系统，展示时对银行卡号进行了屏蔽展示，但手机号、证件号、姓名未进行屏蔽展示。	部分符合	XYSJ-001
	在个人金融信息共享和转让前，应开展个人金融信息接收方信息安全保障能力评估，并与其签署数据保护责任承诺。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业 务），不涉及个人金融信息的共享和转让，故此检测项不适用。	不适用	
	应向个人金融信息主体告知共享、转让个人金融信息的目的、个人金融信息接收方的类型，并事先征得个人金融信息主体明示同意。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业 务），不涉及个人金融信息的共享和转让，故此检测项不适用。	不适用	
	支付账号及其等效信息在共享和转让时，除法律法规和	融通保以应用系统方式为金融机构供应链	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
	行业主管部门另有规定外，应使用支付标记化（按照JR/T0149）技术进行脱敏处理（因业务需要无法使用支付标记化技术时，应进行加密），防范个人金融信息泄露风险。	链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业 务），不涉及个人金融信息的共享和转让，故此检测项不适用。		
	应执行严格的审核程序，并准确记录和保存个人金融信息共享和转让情况。记录内容应包括但不限于日期、规模、目的、范围，以及个人金融信息接收方基本情况与使用意图等，并应确保对共享和转让的个人金融信息及其过程可被追溯。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业 务），不涉及个人金融信息的共享和转让，故此检测项不适用。	不适用	
	在个人金融信息共享和转让的过程中，应部署信息防泄露监控工具，监控及报告个人金融信息的违规外发行为。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业 务），不涉及个人金融信息的共享和转让，故此检测项不适用。	不适用	
	个人金融信息原则上不得公开披露，经法律授权或具备合理事由确需公开披露时，应事先开展个人金融信息安全影响评估，准确记录和保存个人金融信息的公开披露情况，包括公开披露的日期、规模、目的、内容、公开范围等。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业 务），不涉及个人金融信息的公开披露，故此检测项不适用。	不适用	
	因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（包含外包服务机构与外部合作机构）处理时，应采用去标识化（不应仅使用加密技术）等方式进行脱敏处理，降低个人金	申请机构通过融通保系统收集个人信息（非个人金融信息），为内部收集，未委托或授权其它机构收集个人信息，故此检测项不适用。	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
	融信息被泄露、误用、滥用的风险。			
	应对委托行为进行个人金融信息安全影响评估，并确保受委托者具备足够的数据安全能力，且提供了足够的安全保护措施。	申请机构通过融通保系统收集个人信息（非个人金融信息），为内部收集，未委托或授权其它机构收集个人信息。	符合	
	在个人金融信息加工处理的过程中，应建立个人金融信息防泄露控制规范和机制，防止个人金融信息处理过程中的调试信息、日志记录等因不受控制的输出而泄露受保护的信息。	申请机构具有《兴业银行集团个人信息保护管理办法》个人信息使用章节有“各单位应充分梳理所辖个人信息的使用场景，按“最小必需”原则规划设计相关业务流程和岗位，制定个人信息使用的操作制度和规程，有效降低个人信息的暴露面”的描述。	符合	
	在个人金融信息开发测试过程中，应对开发测试环境与生产环境进行有效隔离。	经访谈技术负责人，开发测试环境与生产环境是完全独立的两套环境，二者进行了物流隔离，属于不同的网段。	符合	
	开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化（不应仅使用加密技术）脱敏处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需个人金融信息除外。	经访谈技术负责人，开发环境、测试环境数据均为虚拟数据（虚假数据生成器生成的数据），未使用真实的个人金融信息。	符合	
	汇聚融合的个人金融信息不应超出收集时所声明的使用范围。因业务需要确需超范围使用的，应再次征得个人金融信息主体明示同意。	申请机构所收集的信息同注册服务协议中描述一致，未超出收集时所声明的使用范围。	符合	
删除	应采取技术手段，在金融产品和服务所涉及的系统中去	申请机构对于数据处理有严格管理办法，增	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	除个人金融信息，使其保持不可被检索和访问。	删改查均有相应授权流程；经访谈技术人员，每次退出融通保系统，均会删除内存中个人金融信息。		
销毁	应对个人金融信息存储介质销毁过程进行监督与控制，对待销毁介质的登记、审批、介质交接、销毁执行等过程进行监督。	申请机构具有《兴业银行集团个人信息保护管理办法》，文档中第六节有个人信息删除与销毁有此描述。	符合	

4.1.2 安全管理

测评对象	测评指标	结果记录	结果判定	问题编号
安全策略	应建立个人金融信息保护制度体系，明确工作职责，规范工作流程。制度体系的管理范畴应涵盖本机构、外包服务机构与外部合作机构，并确保相关制度发布并传达给本机构员工及外部合作方（包括外包服务机构、外部合作机构）。相关制度应至少包括个人金融信息保护管理规定、日常管理及操作流程、外包服务机构与外部合作机构管理、内外部检查及监督机制、应急处理流程和预案、个人金融信息投诉与申诉处理程序。	申请机构已建立了个人金融信息保护制度《兴业银行集团个人信息保护管理办法》、《融通保_外包管理办法》、《兴业银行集团信息安全事件应急处置规程》、《兴业银行信息科技系统突发事件应急处置细则》、《云客服服务业务处理流程》、《服务规范和投诉应急方案》，文档中包括了个人金融信息保护管理规定、日常管理及操作流程、外包服务机构与外部合作机构管理、内外部检查及监督机制、应急处理流程和预案、个人金融信息投诉与申诉处理程序等内容的描述。	符合	
	应明确个人金融信息保护责任人和个人金融信息保护有关责任机构，并明确工作职责及工作流程。	《兴业银行集团个人信息保护管理办法》中第二章“职责分工”有个人金融信息保护责	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		任人和个人金融信息保护有关责任机构，并明确工作职责及工作流程的描述。		
	应定期（至少每年一次）或在隐私政策发生重大变化时，对个人金融信息处理岗位上的相关人员开展个人金融信息安全专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程。	《兴业银行集团个人信息保护管理办法》规定各单位应至少每年开展一次面向全体员工的个人信息保护意识宣贯，并提供了培训记录。	符合	
访问控制	应对个人金融信息使用的权限管理应设置权限指派、回收、过期处理等安全功能。	融通保后台管理系统可以对登录用户进行权限分配、收回等操作，不同角色的用户权限不一样。	符合	
	对于可访问和处理个人金融信息的系统应设置基于角色的访问控制策略，对系统用户个人金融信息的增删改查等操作进行记录，保证操作日志的完备性、可用性及可追溯性，操作日志包括但不限于业务操作日志、系统日志等，并要求系统运维管理类日志不应记录个人金融信息。	融通保后台管理系统可以对登录用户进行权限分配、收回等操作，不同角色的用户权限不一样；系统日志分为业务处操作日志、系统运维日志，日志均保存在日志服务器上。	符合	
监测评估	应定期对涉及个人金融信息的信息系统进行安全检查和评估，特别是对于个人金融信息中的支付信息部分，应采取自行评估或委托外部机构进行检查评估，本机构以及与其合作的外部合作方（包括外包服务机构、外部合作机构）应每年至少开展一次支付信息安全合规评估，对评估过程中发现的问题及时	融通保系统以应用系统方式向金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业 务），不涉及支付信息，故此项不适用。	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
	采取补救措施并形成报告存档备查。			
	应采取技术手段对个人金融信息全生命周期进行安全风险识别和管控，如恶意代码检测、异常流量监测、用户行为分析等。	申请机构部署了Pingpoint、SMARTBI对异常流量、用户行为进行监控，以进行风险识别。	符合	
事件处置	应制定个人金融信息安全事件应急预案，明确安全事件处置流程和岗位职责，并定期组织内部相关人员进行个人金融信息保护应急预案相关培训和应急演练。	《兴业银行信息科技系统突发事件应急处置细则》中有组织机构与职责、应急预案与演练的描述，并提供了应急演练预案。	符合	
	应建立投诉与申诉管理机制，包括跟踪流程，并在规定的时间内，对投诉、申诉进行响应。	申请机构制定了《服务规范和投诉应急方案》、《云客服服务业务处理流程》；文档中有规定的时间内进行投诉、申诉的描述。	符合	

4.2 交易安全

测评对象	测评指标	结果记录	结果判定	问题编号
交易验证	交易验证应组合选用下列三类要素：仅客户本人知悉的要素，如静态密码等；仅客户本人持有并特有的，不可复制或者不可重复利用的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等；客户本人生物特性要素，如指纹、虹膜、声纹等。	票据买方、卖方签署协议上链成功后，若是线上交易的话，需买方进行线上交易，买方操作员输入手机号、登录密码、短信验证码登录到执剑人系统，选择相应的订单，输入支付密码后，该笔订单支付成功。	符合	
	申请机构应确保采用的要素相互独立，即部分要素的损坏或者泄露不应导致其他要素损坏或者泄露。	票据买方、卖方签署协议上链成功后，若是线上交易的话，需买方进行线上交易，买方操	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		作员输入手机号、登录密码、短信验证码登录到执剑人系统，选择相应的订单，输入支付密码后，该笔订单支付成功，登录密码、手机验证码、支付密码三者相互独立。		
	申请机构应严格限制使用初始交易密码并提示客户及时修改，建立交易密码复杂度校验机制，避免交易密码过于简单（如“111111”、“123456”等）或与个人金融信息（如出生日期、证件号码、手机号码等）相似度过高。	经查看系统，建立了登录密码复杂度校验机制，登录密码必须为英文大小写、数字、特殊字符的组合，最短 6 位；支付密码为 6 位数字，输入时自带小键盘随机。	符合	
	申请机构采用数字证书、电子签名作为认证要素的，数字证书及生成电子签名的过程应符合《中华人民共和国电子签名法》、JR/T0118 等有关规定，确保数字证书的唯一性、完整性及交易的抗抵赖性。	买卖双方签约（电子合同）的环节会自动使用底层服务倚天鉴，生成电子签章(CFCA 生成的电子证书），电子签章生成的过程符合《中华人民共和国电子签名法》、JR/T 0118 等有关规定。	符合	
	申请机构采用一次性密码作为验证要素的，应切实防范一次性密码获取端与交易指令发起端为相同物理设备而带来的风险，并将一次性密码有效期严格限制在最短的必要时间内。	票据买方、卖方签署协议上链成功后，若是线上交易的话，需买方进行线上交易，买方操作员输入手机号、登录密码、短信验证码登录到执剑人系统，选择相应的订单，输入支付密码后，该笔订单支	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
		付成功，无一次性密码的场景，故检测项不适用。		
	申请机构采用客户本人生物特征作为验证要素的，应符合国家、金融行业标准和相关信息安全管理要求，防止被非法存储、复制或重放。	票据买方、卖方签署协议上链成功后，若是线上交易的话，需买方进行线上交易，买方操作员输入手机号、登录密码、短信验证码登录到执剑人系统，选择相应的订单，输入支付密码后，该笔订单支付成功，无个人生物特征的场景，故检测项不适用。	不适用	
	申请机构应经过客户确认并进行交易验证，交易验证宜同时采用上述三类要素中的两类要素，不足两类的应采取相应的风险补偿措施。	票据买方、卖方签署协议上链成功后，若是线上交易的话，需买方进行线上交易，买方操作员输入手机号、登录密码、短信验证码登录到执剑人系统，选择相应的订单，输入支付密码后，该笔订单支付成功。	符合	
	进行支付交易时，申请机构应采取交易验证强度与交易额度相匹配的技术措施，提高交易的安全性。	票据买方、卖方签署协议上链成功后，若是线上交易的话，需买方进行线上交易，买方操作员输入手机号、登录密码、短信验证码登录到执剑人系统，选择相应的订单，输入支付密码后，该笔订单方可支付成功。	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
交易确认	申请机构应根据客户意愿，为其提供开通或关闭支付服务。	客户通过融通保平台进行注册时，可自愿开通线上交易功能；开通后，在客户提出申请的情况下，后台运维人员可进行关闭。	符合	
	进行智能支付时，申请机构应采用支付口令或其他可靠的技术手段（不适用国家统一推行的金融科技产品认证）实现本人主动确权，保障用户的知情权、财产安全权等合法权益。	票据买方、卖方签署协议上链成功后，若是线上交易的话，需买方进行线上交易，买方操作员输入手机号、登录密码、短信验证码登录到执剑人系统，选择相应的订单，输入支付密码后，该笔订单支付成功。	符合	
	申请机构应采取有效措施，确保客户在执行支付指令前可对收付款客户名称和账号、交易金额等交易信息进行确认，并在支付指令完成后展现交易信息或及时将结果通知客户。	系统支付前有信息展示及确认操作，支付完成后结果及通知及时通知客户票据买方、卖方签署协议上链成功后，若是线上交易的话，需买方进行线上交易，买方操作员输入手机号、登录密码、短信验证码登录到执剑人系统，选择相应的订单，进行确认，输入支付密码后，该笔订单支付成功，以页面展示方式将结果通知客户。	符合	
	申请机构应确保交易信息的真实性、完整性、可追溯性以及在支付全流程中的一致	客户开始注册、签约、交易，所有的信息都会记录到数	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	性，不得篡改或者隐匿交易信息。	据库，该笔交易有唯一的 ID 保持全流程的一致性，通过该笔交易的日志可以进行追溯。		
交易监控建立	申请机构应建立支付交易监控系统，能够甄别并预警潜在风险的交易，例如套现、洗钱、欺诈等可疑交易，并生成风险监控报告。	申请机构有独立数据交易信息监控模块，以甄别洗钱等可疑交易，公司接入了 SMARTBI（应用层），设置阈值，进行监控，可视化展示并生成报告。	符合	
	申请机构应根据交易的风险特征建立风险交易模型，有效监测可疑交易，对可疑交易建立报告、复核、查结机制。	申请机构部署了 Pingpoint，对可疑交易（频繁 IP 发起的交易）进行监控，发下异常后，后续会有专人进行处跟踪处理。	符合	
大数据风险防控	申请机构应采用大数据分析、客户行为建模等手段，建立交易风险监控模型和系统，对异常交易进行及时预警，并采取调查核实、风险提示、延迟结算等处理措施	申请机构有独立数据交易信息监控模块，以甄别洗钱等可疑交易，公司接入了 SMARTBI（应用层），对异常交易及行为异常的用户，利用 rpa 流程机器人识别异常订单，后续会有专人进行跟踪处理。	符合	
	申请机构应不使用交易行为分析、机器学习等不断优化风险评估模型，提高欺诈交易拦截成功率，切实提升交易安全防护能力。	申请机构有独立数据交易信息监控模块，以甄别洗钱等可疑交易，公司接入了 SMARTBI（应用层）、Pingpoint，对异常交易及行为异常的用户，利用 rpa 流程机器人识别异常订单，后续	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		会有专人进行跟踪处理。		
交易风险控制	申请机构应对监控到的风险交易进行及时分析与处置。	申请机构有独立数据交易信息监控模块，以甄别洗钱等可疑交易，公司接入了 SMARTBI（应用层）、Pingpoint，对异常交易及行为异常的用户，利用 rpa 流程机器人识别异常订单，后续会有专人进行跟踪处理。	符合	
	对于资金类交易等高风险业务，申请机构应在确保客户联系方式有效的前提下，及时告知客户其资金变化情况。	申请机构有独立数据交易信息监控模块，以甄别洗钱等可疑交易，公司接入了 SMARTBI（应用层）、Pingpoint，对异常交易及行为进行监控，会对用户进行实时短信通知。	符合	
	对于超过交易风险提示额度的大额交易、短时高频和短时跨地区等疑似风险交易，申请机构应及时向客户提示交易风险，交易风险提示方式由申请机构与客户协商确定，具体包括交易前电话确认、账户余额实时提醒等。	申请机构对于疑似风险交易，会终止该笔交易，后续有专人核实情况进行后续处理。	符合	
	申请机构应对批量或高频登录等异常行为,利用 IP 地址、终端设备标识等信息进行综合识别，及时采取附加验证、拒绝请求等手段。	对于接入融通保系统的用户均绑定 IP，对于高频操作等异常行为进行鉴别控制。	符合	
	申请机构应建立各类交易的黑白名单验证和管理机制，在黑名单中的应直接拒绝。	申请机构有独立数据交易信息监控模块，以甄别洗钱等可疑交易，公司接	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		入了 SMARTBI（应用层），设置阈值，进行监控，可视化展示并生成报告。		

4.3 网络安全

测评对象	测评指标	结果记录	结果判定	问题编号
仿冒	申请机构的客户端应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业务），不涉及 APP，故此项不适用。	不适用	
	申请机构的客户端应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业务），不涉及 APP，故此项不适用。	不适用	
	申请机构的客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业务），不涉及 APP，故此项不适用。	不适用	
	申请机构应采取渠道监控等措施对仿冒客户端程序进行监测	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业务），不涉及 APP，故此项不适用。	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
钓鱼	申请机构的客户端应用软件或系统应具有防网络钓鱼的功能。	融通保系统通过在页面显示客户预留信息或通过 Host 校验和 Referrer 校验手段进行防钓鱼防范，并与 CNCERT 福建分中心建立互联网仿冒应用监测和处置的合作机制。	符合	
	申请机构应采取防钓鱼网站控件、钓鱼网站监控工具、钓鱼网站发现服务等技术措施，及时监测发现钓鱼网站，并建立钓鱼网站案件报告及快速关闭钓鱼网站的处置机制	融通保系统通过在页面显示客户预留信息或通过 Host 校验和 Referrer 校验手段进行防钓鱼防范，并与 CNCERT 福建分中心建立互联网仿冒应用监测和处置的合作机制；但暂无钓鱼网站监控工具。	部分符合	XYSJ-002
	申请机构应具备防钓鱼的应用控制和风险监控措施。	融通保系统通过在页面显示客户预留信息或通过 Host 校验和 Referrer 校验手段进行防钓鱼防范，并与 CNCERT 福建分中心建立互联网仿冒应用监测和处置的合作机制。	符合	
安全漏洞	申请机构的客户端应用软件应考虑交易处理功能逻辑设计的合理性，避免逻辑漏洞。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业务），不涉及 APP，故此项不适用。	不适用	
	申请机构应具备对处理个人金融信息的系统组件进行实时监测的能力，有效识别和阻止来自内外部的非法访	申请机构对处理个人金融信息的系统组件配置了 waf 工具，并配置相关检	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	问。	测策略，可以对系统进行实时监测并报警，有效识别和阻止来自内外部的非法访问记录。		
	申请机构的 API 和 SDK 应对常见的网络攻击具有安全防护能力。	申请机构对应用系统进行了渗透测试，并提供了渗透测试报告，确保应用系统的安全性。	符合	
	申请机构的移动终端应用 SDK 应具备静态逆向分析防护能力，防范攻击者不适用静态反汇编、字符串分析、导入导出函数识别、配置文件分析等手段获得有关 SDK 实现方式的技术细节。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业务），不涉及 APP，故此项不适用。	不适用	
	申请机构应禁止应用方利用应用程序接口（API）漏洞进行非法操作。	申请机构对应用系统进行了渗透测试，并提供了渗透测试报告，确保应用系统的安全性。	符合	
	申请机构的客户端应用软件应考虑认证、校验等安全保证功能的流程设计的合理性，避免逻辑漏洞。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业务），不涉及 APP，故此项不适用。	不适用	
	申请机构的客户端代码实现应避免调用存在安全漏洞的函数。	融通保以应用系统方式为金融机构供应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业务），不涉及 APP，故此项不适用。	不适用	
	申请机构的客户端程序应考虑客户端程序自身的安全	融通保以应用系统方式为金融机构供	不适用	

测评对象	测评指标	结果记录	结果判定	问题编号
	性，避免代码注入、缓冲区溢出、非法提权等漏洞。	应链链属企业提供票据转让、贴现服务（不涉及企业与企业间票据流转业务），不涉及 APP，故此项不适用。		
	申请机构应对应用程序接口进行源代码安全审计、渗透测试，及时处理安全漏洞，有效控制安全风险。	申请机构对应用系统进行了渗透测试，并提供了渗透测试报告，及时处理安全漏洞，有效控制安全风险。	符合	
	申请机构应进行开源系统或组件的安全评估，及时进行漏洞修复和加固处理。	经访谈技术人员，申请机构研发管理部会定期对组件漏洞进行通报，相关方会针对漏洞进行整改。	符合	
	申请机构的应用系统上线前，应进行程序代码的代码复审，识别可能的后门程序、恶意代码、逻辑缺陷和安全漏洞。	申请机构对应用系统进行了渗透测试，并提供了渗透测试报告，及时处理安全漏洞，有效控制安全风险。	符合	
	申请机构的系统应进行漏洞扫描，及时修补发现的系统安全漏洞。	申请机构进行了漏洞扫描，当发现安全漏洞时，会及时修补，具有漏洞扫描报告、漏洞修复情况表。	符合	
	申请机构的应用系统应建立紧急补丁（应急方案）的开发、发布流程，以备必要时提供紧急补丁或应急方案进行处理，以修补重要安全漏洞。	申请机构提供了《关于开通非工作时间紧急运维处理值班电话的通知》，通知中明确了应用系统运营中断的流程，经申请、审核、合规性检查通过后进行实施，但暂未提供应用系统紧急补丁发布的流程方	部分符合	XYSJ-003

测评对象	测评指标	结果记录	结果判定	问题编号
		案。		
	申请机构的系统应具备对网站页面篡改、网站页面源代码暴露、穷举登录尝试、重放攻击、SQL 注入、跨站脚本攻击、钓鱼、木马以及任意文件上传、下载等已知漏洞的防范能力。	申请机构系统通过 waf 对网站页面篡改、网站页面源代码暴露、穷举登录尝试、重放攻击、SQL 注入、跨站脚本攻击、钓鱼、木马以及任意文件上传、下载等已知漏洞均具有防范能力。	符合	

4.4 业务连续性

测评对象	测评指标	结果记录	结果判定	问题编号
资源配置	申请机构应避免机房采用的多路市电输入均来自于同一个变电站,应对 UPS 等重要设备的报警日志进行及时审核和处理。	申请机构机房采用市电双路，对 UPS 等重要设备进行了监控报警。	符合	
	申请机构应提供冗余通信线路，并选择与主用通信线路不同的电信运营商和不同的物理路径。	申请机构机房采用通联金融科技提供的三线 BGP 线路，三运营商接入（移动、联通、电信），具备冗余通信线路。	符合	
	申请机构核心层、汇聚层的设备和重要的接入层设备均应双机热备，例如，核心交换机、服务器群接入交换机、重要业务管理终端接入交换机、核心路由器、防火墙、均衡负载器、带宽管理器及其他相关重要设备。	经检查网络拓扑图，对网络链路上的各层设备（如接入防火墙、核心交换机、接入交换机、IPS 等）均为双机部署。	符合	
	申请机构 Web 服务器、中间件服务器、前置服务器、数据库服务器等关键数据处理系统均应双机热备或多机集	申请机构产品部署于兴业数金私有云上，云平台为分布式架构，存储为分	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	群，并设置磁盘冗余阵列或分布式多副本存储技术，以避免单一部件故障影响设备运行的风险。	布式三副本，天然具备高冗余性，可以避免单一部件故障影响设备运行的风险。		
	申请机构应梳理并维护关键的设备部件、备件清单，采取有效的措施防止因单个设备部件出现故障，导致冗余设备无法正常启用或切换的风险。	申请机构产品部署于兴业数金私有云上，云平台为分布式架构高冗余，具备高抗故障风险能力。	符合	
	申请机构灾备系统在数据同步的机制和技术架构上不应存在明显的缺陷。	申请机构进行了生产灾备切换演练，并提供了切换演练报告，数据同步的机制和技术架构上不应存在明显的缺陷。	符合	
应急预案及演练	申请机构应建立业务连续性预案程序，预案应包括应急和系统灾难恢复两部分。应急部分包括但不限于灾难场景和范围定义、应急的管理机构和决策机制、应急响应的流程、工具和工作制度等内容。系统灾难恢复部分包括但不限于灾难恢复的范围和目标、灾难恢复的总体规程、各系统恢复的切换步骤、操作手册和业务功能恢复验证测试方法等内容。	申请机构制定了《兴业数字金融服务（上海）股份有限公司业务连续性管理办法》、《兴业数字金融服务（上海）股份有限公司托管业务系统业务连续性计划》、《兴业数字金融服务（上海）股份有限公司业务连续性总体应急预案管理办法》，包括应急和系统灾难恢复两部分。明确了应急和系统灾难恢复两部分包含的内容。	符合	
	申请机构应建立应急预案演练制度，定期组织有业务部门参与的桌面演练和生产系统实战演练，定期对双机热备系统进行切换演练，备份	经查看灾备演练预案，申请机构在年初就制定出了演练方案，包括主备机器、主备线路、同	部分符合	XYSJ-004

测评对象	测评指标	结果记录	结果判定	问题编号
	系统与生产系统的切换要至少每年演练一次。针对 DDoS、网络钓鱼等重要安全威胁，定期开展有相关单位、部门参与的联合演练。	城灾备、数据主备机等内容； 但对于 DDoS、网络钓鱼等重要安全威胁，暂未开展有相关单位、部门参与的联合演练。		
	申请机构应急和灾难恢复流程不应引入数据泄露的风险。	《兴业数字金融服务（上海）股份有限公司业务连续性总体应急预案管理办法》，应急和灾难恢复流程未引入数据泄露的风险。	符合	
备份与恢复管理	申请机构应根据系统的业务影响性分析结果，制定不同数据的备份策略，并实施应用级备份，以保证灾难发生时，能尽快恢复业务运营。	申请机构制定了《兴业数字金融服务股份有限公司生产数据管理规定》，文档中有核心数据和非核心数据备份策略的描述，制定了不同数据的备份策略。	符合	
	申请机构应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存，明确规定备份数据的保存期，做好备份数据的销毁申请、审查和登记工作。	《兴业数字金融服务股份有限公司生产数据管理规定》第六节“备份数据的管理与使用”中有永久保存的备份数据在质量保证期 5 年内进行必要的转储的描述，第四章有‘生产数据的销毁’的描述。	符合	
	申请机构应定期执行恢复程序，检查并测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。	申请机构制定了《兴业数金数据备份策略》，该文档中有核心系统的备份数据至少每年进行一次数据恢复验证测试、非核心系	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		统的备份数据每年抽样进行验证测试的描述。		
	申请机构应对技术方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果，以满足灾难恢复策略的要求。	申请机构提供了《兴业银行 NBU 备份恢复演练报告》，会定期进行恢复演练，对关键技术应用进行了可行性验证测试。	符合	
	申请机构应在统一的灾难恢复策略下建立完善的系统灾难恢复体系，开展灾难恢复需求分析、策略及计划制定、灾备系统建设及演练等工作，并根据实际情况对其进行分析和改进，确保各环节的正确性以及灾难恢复体系的有效性。	申请机构制定了《兴业数金数据备份策略》、《兴业数字金融服务股份有限公司生产数据管理规定》，建立了完善的系统灾难恢复体系。	符合	
	申请机构的同城数据备份中心，应保证可以接管所有核心业务的运行，与生产中心直线距离应满足 JR/T 0071 相关安全技术要求。	申请机构同城备份中心位于上海市华京路 6 号万国数据。	符合	
	申请机构的异地数据备份中心，与生产中心直线距离应满足 JR/T 0071 相关安全技术要求。	申请机构暂无异地备份中心。	不符合	XYSJ-005
安全事件处理	申请机构对于重大信息安全事件，相关人员应注意保护事件现场，采取必要的控制措施。	申请机构制定了《兴业银行信息科技系统突发事件应急处置细则》，第五章节“事件处置”有“信息系统突发事件发生后，各小组成员在接到通知后，应立即赶赴事件现场，参加应急处置工作”的描述。	符合	
	申请机构应定期对本机构及同业发生的信息安全事件及	申请机构依托兴业银行集团获取信息	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	风险进行深入研判、分析，评估现有控制措施的脆弱性，及时整改发现的问题。	安全情报及软硬件重大安全缺陷，系统每年定期开展渗透测试，并第一时间对发现的漏洞问题进行修复，直至漏洞修复测通过。		
监管管理	申请机构应实时监控生产中心和灾备中心的业务应用可用性和性能状态，并具备告警功能。	申请机构云基础服务使用数金互金云平台，集成了zabbix 服务，监视各种网络参数，通过邮件和短信提醒责任人服务器异常状态；本系统集成了 pinpoint 调用链系统、flume 日志收集系统，实时排查和收集应用运行情况。	符合	
	申请机构应能够有效监控灾备切换过程和同步状态。	申请机构数据库使用爱可生管理控台，实时监测数据库运行情况，实时调整数据库运行参数以及主从切换、备份还原等操作。	符合	
管理要求	申请机构应制定业务系统业务连续性策略及计划。	申请机构制定了《兴业数字金融服务（上海）股份有限公司业务连续性管理办法》、《兴业数字金融服务（上海）股份有限公司托管业务系统业务连续性计划》、《兴业数字金融服务（上海）股份有限公司业务连续性总体应急预案管理办法》。	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	申请机构应将业务连续性管理整合到组织的流程和架构中，明确指定相关部门负责业务连续性的管理。	《兴业数字金融服务（上海）股份有限公司业务连续性管理办法》第一节“日常管理组织架构”有相关部门负责业务连续性的管理的描述。	符合	
	申请机构应制定员工在业务连续性方面的培训计划和考核标准。	申请机构提供了连续性培训记录《集团科技人员 ALOPS 培训》，但暂未制定员工在业务连续性方面的培训计划和考核标准。	部分符合	XYSJ-006
	申请机构应定期或在业务系统发生显著变化时，测试并更新业务连续性计划与过程，以确保其持续有效。	申请机构制定了《兴业数字金融服务（上海）股份有限公司业务连续性管理办法》、《兴业数字金融服务（上海）股份有限公司托管业务系统业务连续性计划》、《兴业数字金融服务（上海）股份有限公司业务连续性总体应急预案管理办法》；经访谈，业务系统发生显著变化时，申请机构会测试并更新业务连续性计划与过程，以确保其持续有效。	符合	
	申请机构应至少每年组织一次业务连续性专项内部审计或委托第三方进行的审计，并形成包括审计意见、改进计划和改进结果的审计报告。	申请机构暂未进行业务连续性专项审计。	不符合	XYSJ-007

4.5 技术使用安全

4.5.1 区块链(基础版)

测评对象	测评指标	结果记录	结果判定	问题编号
基础环境安全	基础硬件和软件环境应遵循《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）中三级及以上的物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复相关要求	区块链暂不具备安全的基础环境，暂未进行等级保护的安全评估。	不符合	XYSJ-008
密码算法安全	分布式账本系统所使用的具体密码算法应符合密码相关国家标准、行业标准的有关要求，并应使用符合相关国家标准、行业标准的密码模块完成密码算法运算和密钥存储。	1.经过openssl命令对tls通讯证书核查，通信过程中对业务数据进行加密传输，经查看版本为tls1.2通讯协议x509 v3格式证书； 2.经查看业务代码，业务层使用RSA算法加密； 3.区块链使用的对称密码算法为AES(业务数据加密),非对称密码算法为ECDSA(数字签名、公钥加密和密钥交换)，哈希算法为SHA256(摘要算法，生成256bit的摘要)； 4.SDK发起一笔请求，查看日志信息：交易发起者用私钥对交易数据进行数字签名，网关服务在收到请求后会使用交易发起者的公钥对其进行验证，验证通过后，会用私钥对该笔请求进行数字签名，并将该笔请求广播到共识节点，通过数字签名保证了数据完整性。	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
节点通信安全	应对分布式账本系统采取授权准入的原则，在节点通信过程中应保证数据的完整性和保密性。应采用密码技术对节点通信双方的身份进行验证。	1. 兴业数金区块链的节点采用 tls 双向认证，经查看 tls 版本 tls1.2； 2.区块链使用的对称密码算法为 AES(业务数据加密),非对称密码算法为 ECDSA(数字签名、公钥加密和密钥交换)，哈希算法为 SHA256(摘要算法，生成 256bit 的摘要)； 3.模拟该节点无 CA 证书，启动该节点，节点启动失败，经查志信息，显示‘certificate has expired or is not yet valid.’；给节点配置正确的 CA 证书，启动该节点，可以正常启动成功； 4.SDK 无 CA 证书时，启动 console（console 通过 sdk 连接区块链），启动失败，无法连接到区块链节点；给 SDK 配置正确的证书，启动 console,可以正常启动成功； 5.SDK 发起一笔请求，查看日志信息：交易发起者用私钥对交易数据进行数字签名，网关服务在收到请求后会使用交易发起者的公钥对其进行验证，验证通过后，会用私钥对该笔请求进行数字签名，以此保证通信完整性。	符合	
账本数据安全	应对账本数据进行冗余，并确保账本数据不被未经	1. 兴业数金平台发起一笔请求，该请求上链	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	授权方获取，保证账本数据的完整性、一致性和保密性。应对账本数据的访问提供安全审计功能。	成功，查看各共识节点账本数据，该笔请求上链成功，各节点数据一致； 2.将一个节点的账本文件修改，修改完成后，发起一笔交易；经查看该节点的日志信息，由于背书策略中该节点验证失败，导致交易失败； 3.兴业数金区块链 BAAS 平台，对账本数据的访问提供安全审计，存证业务中具体账本数据的新增、查询等； 4.手工新加入一个节点，对该节点进行相应的配置，成功启动后，查看日志信息，日志中会记录从其它几点同步账本数据，查看账本数据文件，新加入节点的账本文件与其它节点一致； 5.SDK 发起一笔请求，该笔请求上链成功后，查看账本文件，该笔请求有发起者的签名信息。		
共识协议安全	应根据业务特点选用适宜的共识协议，包括但不限于工作量证明、权益证明、授权股权证明、拜占庭容错等，应满足不同共识协议安全运行所必需的前提要求，且业务激励规则和技术运维安全上的机制设计应保障其自身安全。	1.经访谈技术人员，产品的区块链采用 RAFT 共识协议：网关服务将请求随机发送到一个节点，该节点将请求广播到各节点，Leader 节点收到请求，轮询时间到达后，从交易池中获取交易，并将获取的交易插入到产生的新区块，并将新区块广播	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		给组内所有共识节点，共识节点向主节点返回验证消息，若返回的验证消息大于等于 2，则提交该区块，写入数据库，共识达成一致； 2.共识协议算法运行环境具备安全性与可靠性，且运行环境进行过等保测评，并提供了等保测评报告； 3.经查看共识节点日志，共识算法完成时间小于 1 秒； 4.产品的区块链有 3 个 order 节点，且可以正常处理请求；手动添加或删除一个 order 节点的过程中，发起 API 请求，API 请求可以共识成功，查看各 peer 节点账本信息一致； 5.发起一笔 API 请求，该请求会发送到共识节点，查看共识节点的日志，日志会打印出该笔请求的共识过程；节点的日志会同步到数据库； 6.停下 2 个节点，发起交易，经查看日志，该笔交易异常，未成功出块。		
智能合约安全	可支持图灵完备合约，交易信息中应明确调用的 evidence 合约版本。	1. evidence 合约有相应的注册机制，注册过的组织成员才可以部署和调用合约（群组中的节点都可以看到合约，不一定能调用合约，需要注册后才能访问），未进行注册的私	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		钥证书不能能进行查询操作，也不能进行调用； 2.经查看产品的 evidence 合约源码，采用 golang 语言编写，为图灵完备合约；图 52 3. evidence 合约部署完成后，会成功上链； 4.在发起的请求中，会有相应 evidence 合约的名字，以确定调用相应的 evidence 合约； 5.发起一笔 API 请求，该笔请求上链成功后，查看各节点的账本信息，该笔请求的写集一致； 6. evidence 合约全生命周期包含：打包（Package）、安装（Install）、实例化（Instantiate）、运行（Running）以及升级（Upgrade）。		
身份管理安全	应根据金融业务需求制定身份数据保密性要求，确保数据不暴露给未经授权方。监管信息应至少包括金融监管信息，具体为现工作单位/就读学校、行业类型、居住国家/地区、民族、居民/非居民、出生日期、个人月收入、税务信息等监管数据项和反洗钱特色数据项。	1.根证书向节点发行节点证书，节点证书中的公钥为节点的唯一身份； 2.兴业数金具备客户监管信息的方法和手段，给监管机构预留了接口，以 WEBSOCKET 方式主动推送该监管机构。	符合	
安全运维与治理	应符合《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）中安全管理制度、管理机构、人员安全、运维管理	1.申请机构通过 zabbix 对节点状态进行监控，当节点状态异常时，会通过短信进行报警；	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	相关要求，同时还应包括设备管理、节点监控、节点版本升级、漏洞修复、备份与恢复、应急预案管理、权限管理、议案机制等功能。	2.申请机构提供了《兴业数字金融服务（上海）股份有限公司业务连续性总体应急预案管理办法》； 3.申请机构提供了《兴业数金数据备份策略》。		

4.5.2 云计算

测评对象	测评指标	结果记录	结果判定	问题编号
计算池资源	应支持多虚拟机管理与配置。	云计算平台采用 openstack 技术使用 kvm 实现虚拟化，能够支持多虚拟机的管理与配置。	符合	
计算池资源	应支持动态增加虚拟机 CPU、内存的配置，满足业务运行需求。	云计算平台采用 openstack 技术使用 kvm 实现虚拟化，能够对运行的虚拟机动态增加 CPU、内存配置，满足业务运行需求。	符合	
计算池资源	应支持计算资源池化，提供可动态调整的 CPU、内存、I/O 设备等资源。	云计算平台采用 openstack 技术使用 kvm 实现虚拟化，支持计算资源池化，能够动态调整 CPU、内存资源。	符合	
计算池资源	应支持计算资源灵活调配的功能。	云计算平台采用 openstack 技术使用 kvm 实现虚拟化，支持计算资源灵活调配。	符合	
计算池资源	应支持根据资源使用情况自动伸缩资源。	云计算平台采用 openstack 技术使用 kvm 实现虚拟化，能够实现根据资源使用情况自动伸缩资源。	符合	
计算池资源	应支持运行状态下的虚拟机动态迁移，并维持业务正常运行。	云计算平台采用 openstack 技术，支持虚拟机在运行状态下	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
		的热迁移，能够维持业务正常运行。		
存储系统	应支持存储系统在线扩容和自动数据平衡。	云计算平台采用 openstack 技术，支持存储系统的在线扩容和自动数据平衡。	符合	
存储系统	应支持云服务使用者访问存储资源的安全传输。	云计算平台采用 rbd 的 safe 安全协议访问存储资源，能够支持存储资源的安全传输。	符合	
存储资源池安全	应支持内容加密存储，加密密钥支持云服务使用者自管理、云服务提供者管理和第三方机构管理。	云计算平台采用 rbd 的 safe 安全协议对数据拆分存储，以数据碎片的方式分别存储。内容加密存储由应用端实现。	符合	
计算资源安全-访问控制	应对访问主体进行必要的身份验证。	云计算平台对云服务用户采用口令验证用户身份，应用服务器访问存储资源采用 token 实现身份验证。	符合	

4.6 内控管理

测评对象	测评指标	结果记录	结果判定	问题编号
内控管理	申请机构应结合当前的法规政策、标准规范、应用模式、服务产品、信息系统支撑等方面，结合自身工作基础，说明金融科技应用的必要性、可行性。	申请机构制定了《融通保_金融科技创新应用内控管理制度》，该文档中有金融科技应用的必要性、可行性的描述。	符合	
	申请机构应对金融科技应用的具体目标、预期效果提出可量化的指标。	申请机构制定了《融通保_金融科技创新应用内控管理制度》，文档中固有“预计上线后年服务企业 1000 家，年流转票据 2 万笔，年流转规模 200 亿。”的描述。	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	申请机构应明确金融科技应用的业务功能、服务对象、预期用户规模和应用模式，说明金融科技应用采用的主要技术。	申请机构制定了《融通保_金融科技创新应用内控管理制度》，“技术应用”章节有金融科技应用采用的主要技术的描述。	符合	
	申请机构应做好新技术金融应用风险防范。充分评估新技术与业务融合的潜在风险，建立健全试错容错机制，完善风险拨备资金、保险计划、应急处置等风险补偿措施。具体要求如下：申请机构应根据新技术与业务融合的潜在风险，制定风险拨备资金管理要求；申请机构应根据新技术与业务融合的潜在风险，完善保险计划；申请机构应具备先行赔付、保险补偿等保护金融消费者合法权益的具体措施；申请机构应根据新技术与业务融合的潜在风险，完善应急处置措施；申请机构应具备重大突发事件应急处置机制。	申请制定了《融通保系统应急预案》、《融通保风险补偿机制》、《兴业银行信息科技系统突发事件应急处置细则》、《兴业银行集团信息安全事件应急处置规程》，充分评估新技术与业务融合的潜在风险，建立健全试错容错机制，完善风险拨备资金、保险计划、应急处置等风险补偿措施。	符合	
	申请机构应制定金融科技应用的运营策略。	申请机构制定了运营策略，包含融通保详解、融通保面临的问题、融通保发展的目标、市场客户需求、融通保需要的补偿和创新等运营策略。	符合	
	申请机构应明确金融科技应用的工作组织机制，明确工作负责人。金融科技应用由多个机构共同开发、运营时，应指定牵头负责单位，建立工作协调	申请机构提供了各部门组织架构及职能分工，明确了金融科技应用的工作组织机制及工作负责人。	符合	

测评对象	测评指标	结果记录	结果判定	问题编号
	机制、联合运营机制、问题协同处理机制等控制措施			
	申请机构应定期开展金融科技应用内部审计。	经访谈人员，申请机构每年进行1次金融科技应用内部设计，并提供了内部审计报告。	符合	
	申请机构应在金融科技应用上线前开展外部安全评估，并形成报告备查。	申请机构对金融科技应用进行了渗透测试，提供了渗透测试报告《兴业数金聚票盈平台管理端系统渗透测试报告》、《兴业数金聚票盈平台渗透测试报告 0190521》。	符合	

5. 评估总结

5.1 评估过程描述

针对兴业数字金融服务（上海）股份有限公司“融通保”中小微企业票据流转支持产品，按照《金融科技创新安全通用规范（试行）》要求，在兴业数字金融服务（上海）股份有限公司搭建的环境中进行了全面的检测，此次检测内容主要包括信息保护、交易安全、网络安全、业务连续性、区块链(基础版)、云计算、内控管理等七个方面，并得出了相关的检测结果，但对于升级、与软硬件环境关系密切和没有检测到的业务等不在此次检测说明范围内。

5.2 评估总结

根据《金融科技创新安全通用规范（试行）》判定结果如下：

信息保护检测：共包含 37 个检测项，实际检测 25 个检测项，判定结果为“符合”的有 23 项，判定结果为“部分符合”的有 2 项，无判定结果为“不符合”的项，判定结果为“不适用”的有 12 项。

交易安全检测：共包含 21 个检测项，实际检测 19 个检测项，判定结果为“符合”的有 19 项，无判定结果为“部分符合”和“不符合”的项，判定结果为“不

适用”的有 2 项。

网络安全检测：共包含 21 个检测项，实际检测 12 个检测项，判定结果为“符合”的有 10 项，判定结果为“部分符合”的有 2 项，无判定结果为“不符合”的项，判定结果为“不适用”的有 9 项。

业务连续性检测：共包含 25 个检测项，实际检测 25 个检测项，判定结果为“符合”的有 21 项，判定结果为“部分符合”的有 2 项，判定结果为“不符合”的有 2 项，无判定结果为“不适用”的项。

云计算检测：共包含 10 个检测项，实际检测 10 个检测项，判定结果为“符合”的有 10 项，无判定结果为“部分符合”、“不符合”和“不适用”的项。

区块链(基础版)检测：共包含 8 个检测项，实际检测 8 个检测项，判定结果为“符合”的有 7 项，判定结果为“不符合”的有 1 项，无判定结果为“部分符合”和“不适用”的项。

内控管理检测：共包含 8 个检测项，实际检测 8 个检测项，判定结果为“符合”的有 8 项，无判定结果为“不符合”、“部分符合”和“不适用”的项。

本次技术性安全评估共包含 130 个检测项，实际检测 107 个检测项，其中判定结果为“符合”的有 98 项，判定结果为“部分符合”的有 6 项，判定结果为“不符合”的有 3 项，判定结果为“不适用”的有 23 项。

具体检测情况及结果如下表所示：

序号	检测项						
	名称	检测项	实际检测项	符合项	部分符合项	不符合项	不适用项
1	信息保护	37	25	23	2	0	12
2	交易安全	21	19	19	0	0	2
3	网络安全	21	12	10	2	0	9
4	业务连续性	25	25	21	2	2	0
5	云计算	10	10	10	0	0	0
6	区块链(基础版)	8	8	7	0	1	0
7	内控管理	8	8	8	0	0	0

序号	检测项						
	名称	检测项	实际检测项	符合项	部分符合项	不符合项	不适用项
综合		130	107	98	6	3	23

5.3 问题列表

问题编号	问题描述	测评对象	整改情况
XYSJ-001	融通保系统在用户注册签约时，会收集用户的手机号、证件号、银行卡号、银行行号、所属银行信息，展示时对银行卡号就行了屏蔽展示，但手机号、证件号、姓名未进行屏蔽展示。 补救措施：申请机构承诺六个月内对应用进行整改。	信息保护	限期整改
XYSJ-002	融通保系统暂无钓鱼网站监控工具。 补救措施：通保系统通过在页面显示客户预留信息或通过 Host 校验和 Referrer 校验手段进行防钓鱼防范，并承诺六个月内部署防钓鱼网站监控工具。	网络安全	限期整改
XYSJ-003	申请机构暂未提供应用系统紧急补丁发布的流程方案。 补救措施：申请机构提供了《关于开通非工作时间紧急运维处理值班电话的通知》，通知中明确了应用系统运营中断的流程，并承诺六个月内制定申请机构提供了《关于开通非工作时间紧急运维处理值班电话的通知》，通知中明确了应用系统运营中断的流程。	网络安全	限期整改
XYSJ-004	申请机构对于 DDoS、网络钓鱼等重要安全威胁，暂未开展有相关单位、部门参与的联合演练。 补救措施：申请机构会定期进行预案演练。	业务连续性	长期观察
XYSJ-005	申请机构暂无异地备份中心。 补救措施：申请机构承诺六个月内建立异地备份中心。	业务连续性	限期整改
XYSJ-006	申请机构暂未制定员工在业务连续性方面的培训计划和考核标准。 补救措施：申请机构承诺六个月内制定业务连续性方面的培训计划和考核标准。	业务连续性	长期观察

XYSJ-007	申请机构暂未进行业务连续性专项审计。 补救措施：申请机构承诺六个月内进行业务连续性专项审计，并形成审计报告。	业务连续性	限期整改
XYSJ-008	区块链暂不具备安全的基础环境，暂未进行《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的安全。 补救措施：申请机构承诺六个月内进行等级保护评估。	区块链	限期整改

6. 附件

无。

“融通保”中小微企业票据流转支持产品
风险补偿机制

2020 年 6 月

智慧供应链金融事业部

目录

一、概述

1.1 目的

为保障客户权益，确保因产品的不可以预测问题导致的对客户合法权益造成损害时，最大程度降低用户损失。特制定本细则。

1.2 适用范围

本细则适用于按照业务规则开展业务的客户，因发生系统不可预测问题导致的资金被盗刷、错账等问题，通过“融通保”中小微企业票据流转支持产品投诉渠道提出的风险补偿申诉。

1.3 业务参与方与职责概述

运营主体：运营主体指的是对接“融通保”产品，自主营销客户，运营产品业务的自然人主体。运营主体根据本机制细则要求，协助调查取证和材料收集，对因自身运营、操作、欺诈等造成的问题，应当全面负责并进行相应补偿。

金融机构：金融机构指客户业务处理过程中资金、资产所涉及的金融机构，因金融机构自身变更、缺陷导致的资金、资产问题由金融机构自行处理。

兴业数金：兴业数金指“融通保”产品开发方及运维方-兴业数字金融服务（上海）股份有限公司。接受并核实处理用户正规渠道提出的合理申诉，针对因自身系统设计漏洞产生的客户合法权益受损，基于

此机制进行及时有效的补偿。

二、风险补偿对象

风险补偿对象为合法合规存续且在“融通保”产品认证为“正常”状态，且在业务操作中因不可预测事故导致自身合法权益受到了损害的企业用户。

三、风险补偿原则

风险补偿处理应秉持客户权益优先原则、客观公正原则、及时响应原则，切实保障客户合法权益。

四、风险补偿处理流程

1、企业用户通过“融通保”投诉渠道（电话及邮箱）提出申诉；

2、我司接受投诉人申诉，并按照流程进行调查取证，对申诉者、运营主体本身可能存在的道德风险进行排除性检查；

3、核查清楚申诉者权益损害的事与愿违，依据核查结果交由相关责任方进行风险补偿；

4、对于由于“融通保”系统本身缺陷给客户合法权益带来的损害，应当根据客户已损失合法权益进行协商补偿。10 个工作日内完成补偿。

五、其他事项

出现因申诉人出于欺诈、联合欺诈等手段骗取补偿的，将不予补偿并提交司法部门处理。

“融通保”中小微企业票据流转支持产品退出机制

以市场化、法制化原则按照国家有关法律法规要求，坚持公开透明，最大限度保护各方当事人的合法权益的原则稳妥、有序退出。

一、退出条件

1.因以下任何原因，双方可以终止用户服务：

（1）经同运营主体协商一致，同意终止合作协议，则终止对该租户下用户提供服务；

（2）使用方因自身原因不再继续使用“融通保”产品；

（3）“融通保”产品在运营过程中，遇有不可抗力或其他无法控制的原因造成不能履行或不能完全履行“融通保”相关服务；

（4）因经营策略调整，兴业数字金融服务（上海）股份有限公司将不再继续“融通保”的运营。

2.对下列情形，经双方协商达成一致，可终止合作而不承担违约责任：

（1）法律、法规、规章、政府规范性文件的规定或变动使双方所达成的业务无法继续进行的；

（2）中华人民共和国工业和信息化部、中国人民银行、中国银保监会等监管机构的相关政策调整；

（3）拥有法定监管职责的机构要求立即停止双方所达成的业务的。

二、退出流程

1.兴业数字金融服务（上海）股份有限公司在停止“融通保”产品的运营前，应当按照同合作方的协议所规定的日期，提前以书面、短信、电话等多种形式告知合作方及客户。在进行退出工作时，应确保同时

妥善做好业务和数据的迁移工作、客户的解释工作，并承担合作终止产生的风险和责任。

2.使用者自身自主退出时，任可利用合理渠道联系运营主体以获取自身已取得的合法权益。“融通保”产品正常提供对外服务。

3.数据处理：“融通保”产品将谨遵监管机构的相关监管规定，妥善做好业务、数据以及用户信息的迁移及工作。“融通保”产品所产生业务数据，都采用实时传输的方式储存到核心业务数据库。产品的退出将不会对数据及用户信息产生影响。

4.业务处理：未办结的业务将由运营主体同业务参与者协商办结，用户账户将于推出前完成核查、结清并退出。

“融通保”中小微企业票据流转支持产品系统应急预案

第一章 总则

一、目的

为规范供应链金融事业部信息系统的突发事件应急管理，提高应对突发事件的综合管理水平和应急处置能力，有效防范信息系统风险，结合监管单位要求，特制定“融通保”系统应急预案（以下简称预案）。本预案描述“融通保”系统上线后可能出现的故障场景，以及针对各种故障场景的应急预案及操作步骤。

二、术语和定义

（一） 信息系统

本预案所称信息系统是指由计算机系统、网络系统软硬件及其相关和配套的设备、设施和应用软件等构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、处理和检索等处理的系统。

（二） 突发事件

本预案所称突发事件是指“融通保”系统以及为之提供支持服务的电力、通信等系统突然发生的，影响业务持续开展，需要采取应急处置措施应对的事件。

（三） 信息系统应急预案

信息系统应急预案是指在发生影响信息系统正常运行的紧急事

件或信息系统被破坏后，为更加快速、有效、合理地做出反应，最短时间恢复系统运行，最大程度减少突发事件造成的损失和影响，而预先制订的紧急行动方案。

三、依据

（一）《中华人民共和国突发事件应对法》

（二）《信息系统灾难恢复规范》（GB/T20988-2007）

（三）《银行业信息系统灾难恢复管理规范》（JR/T0044-2008）

（四）《银行业重要信息系统突发事件应急管理规范》（银监办发[2008]53 号）

（五）《中国银监会关于印发商业银行业务连续性监管指引的通知》（银监发[2011]104 号）

四、编制原则

信息系统应急预案编制应遵循以下基本原则：

（一）有效性原则：应急预案应尽可能满足突发事件发生时进行恢复的实际需要，能够及时有效的应对紧急事件，并保持与实际系统和人员组织的同步更新。

（二）可用性原则：应急预案应具有较强的可操作性，包括成本和效率。

（三）高效性原则：应急预案应采用易于理解的语言和图表，高效易用，适合在紧急情况下使用。

（四）完整性原则：应急预案应涵盖应急恢复工作的各个环节，以及应急恢复所需的尽可能全面的数据和资料。

（五）明确性原则：应急预案应采用清晰的结构，对资源及工作内容和步骤进行明确详细的描述，每项工作应有明确的责任人。

五、突发事件应对工作原则

（一）健全机制。建立统一指挥、协调有序的应急管理机制，主动开展应急管理工作，定期演练和评价应急预案，持续改进应急预案和相关协调机制。

（二）明确职责。明确各小组在应急管理工作中的职责，以保障信息系统业务连续性为目标，以落实和完善应急预案为基础，全面加强信息系统应急管理工作。

（三）预防为主。建立和完善信息系统突发事件风险防范体系，对可能导致突发事件的风险进行有效地识别、分析和控制，并对风险指标动态、持续监测，减少重大突发事件发生的可能性。

（四）处置高效。加强应急处置队伍建设，提供充分的资源保障，确保突发事件发生时反应快速、报告及时、措施得力、操作准确，降低突发事件可能造成的损失。

六、适用范围

本预案仅适用于供应链金融事业部在处置“融通保”系统突发事件时采取的技术层面的应急方案，不涉及因业务需求错误、业务误操作等引发的业务层面突发事件。

第二章 应急处置小组

一、应急工作领导小组

应急工作领导小组由我部总经理为组长，总经理助理及各 BU 负责人为组员。应急工作领导小组负责应急处置重大事项的决策、指挥、协调、督导等，联系人名单详见附件 1。

二、应急联系通道建立与维护

应急处置小组具体组成人员名称与联系方式由运营 BU 统一保存维护。应当包含业务联系人 AB 角，技术联系人 AB 角及联系信息。若有人员变更应第一时间更新，同步联系表。

第三章 运营中断预防、检测和预警

一、运营中断预防

- 风险管理宣导培训：合作方上线培训宣导，不定期组织业务运营人员、合作方进行运营风险管理培训，加强各方运营风险重视程度，并使各方知晓应急处置的工作程序与各方职责。对于重要的监管政策与动态，需及时与各方进行必要的信息同步；
- 软件变更管理与验证：“融通保”系统的升级或变更，严格遵循研发管理部对于我司系统变更管理的要求。业务团队至少提前一周告知到各合作方。

二、检测预警机制

1、运行监控策略

系统提供丰富的监控功能，支持系统管理维护人员监控分析系统的运行状态，提供的常规监控管理包括：服务器的管理监控，配置信息管理，运行信息监控，安全访问策略，审计日志查看等功能。

- 系统信息监控:硬件和操作系统信息,JDK信息,应用服务器信息。
- 运行参数信息：数据源配置，消息服务配置。
- 运行统计监控：数据库连接，页面运行情况，SQL运行情况，在线用户等。
- 运行日志信息：页面日志，SQL日志，任务调用日志，服务调用日志。
- 应用信息监控：功能模块使用情况，流程使用情况，服务使用情况等。

2、预警机制

交易检测、主动验证等均有页面预警。预警后第一时间了解具体情况并协调相关人员进行业务应对。

第四章　应急处置程序

一、突发事件分级

突发事件依照其影响范围及故障范围等因素分级。当突发事件同时满足多个级别的定级条件时，按最高级别确定突发事件等级。

（一）严重故障

1、由于系统服务中断或重要数据损毁、丢失、泄露，对银行或客户利益造成严重损害的突发事件；

2、由于系统服务异常，在业务服务时段导致所有功能模块无法正常运行的突发事件；

3、业务服务时段以外，出现的系统故障或事件救治未果，可能产生

上述 1 至 2 类的突发事件。

（二）较大故障

1、由于系统服务中断或重要数据损毁、丢失、泄露，对银行或客户利益造成较大损害的突发事件；

2、由于系统服务异常，在业务服务时段导致核心或重要功能模块无法正常运行的突发事件；

3、业务服务时段以外，出现的系统故障或事件救治未果，可能产生上述 1 至 2 类的突发事件。

（三）一般故障

1、由于系统服务中断或重要数据损毁、丢失、泄露，对银行或客户利益造成轻微损害的突发事件；

2、由于系统服务异常，在业务服务时段导致部分一般功能模块无法正常运行的突发事件；

3、业务服务时段以外，出现的系统故障或事件救治未果，可能产生上述 1 至 2 类的突发事件。

突发事件发生后，应依据事件影响范围和影响时间的变化，按照上述定义进行事件级别分级。

二、应急场景解决方案和应急操作步骤

（一）严重故障场景及解决方案

数据库故障：

1、一旦数据库崩溃，应立即向上级有关部门上报，同时通知暂停系统服务。

2、对主机系统进行修复，如遇到无法解决的问题，应立即向上级单位或软硬件提供商请求支援。

3、修复系统后，将数据库备份取出来，按照要求将其恢复到主机系统中。

4、如果第一个备份损坏，导致无法恢复，则取出下一个数据库备份加以修复。

5、如果所有的备份均无法修复，应立即向有关的厂商请求紧急支援。

服务器故障：

1、服务器发生故障时，应立即向上级有关部门上报，同时根据故障情况确定暂停系统服务或者迁移服务。

2、对主机系统进行修复，如遇到无法解决的问题，应立即向上级单位或软硬件提供商请求支援。

3、修复系统后，将系统备份按照要求将其恢复到主机系统中。

4、如果第一个备份损坏，导致无法恢复，则取出下一个备份加以修复。

5、如果所有的备份均无法修复，应立即向有关的厂商请求紧急支援。

系统上线异常：

系统上线后将进行关联的业务验证。如果业务验证失败，则将系统回退到上一版本。具体回退操作步骤见下文。

资金损失及处理方案：

查明交易信息流、资金流及票据流，及时追回并归还。

（二）较大故障场景及解决方案

系统服务异常导致的用户损失，应在保障客户资金、信息安全无误的前提下及时暂停、检查并整改。

（三）一般故障场景及解决方案

系统业务功能异常：

1、系统将出现异常的交易暂时停用。

2、研发组提交解决方案。

3、研发组进行紧急上线。

4、进行相关功能的验证。

5、验证成功后恢复相关功能。

资金划转异常：

1、暂停当日业务

2、第一时间与总行和公司财务人员联系。

3、验证切换通道是否成功。

4、进行相关功能的验证。

5、验证成功后恢复相关功能。

（四）应急回退操作步骤

1、停止应用

2、数据库表恢复

2.1、备份当前数据库。

2.2、将数据库恢复到前一有效备份。

3、业务验证

4、进行相关的业务验证。

第五章　应急保障

一、系统恢复优先级

系统恢复优先级评定原则：

系统恢复优先级按照“基础环境为本，重要业务优先”的原则。

恢复系统首先是要对基础设施、网络通信等基础环境进行恢复，尤其优先恢复支撑系统运行的基础设施等，保障支撑系统的基础环境可用。应用系统恢复先后顺序根据定义的重要信息系统、安全保护等级，同时考虑系统的时间敏感性等因素进行排定。

二、应急保障

1、物理安全保障：环境安全、设备安全、人员访问控制、异常情况追查等；

2、网络安全保障：网络拓扑结构、网络设备管理严密、网络安全访问管制、不定期安全扫描、远程访问规范化管理等；

3、数据安全保障：数据包括系统运行产生的各种数据，可能存在于文件系统也可能存在于数据库中，这些数据时时刻刻变化的，备份机制要保证能够恢复到故障前的数据状态。

第六章 应急演练

一、演练计划

每年开展至少一次演练，演练重点关注系统故障、网络故障等。在重大业务活动、社会活动等关键时刻的之前及之后，均针对性进行专项演练。

二、演练执行

演练执行包含流程如下：演练启动、演练施行、演练结束。

（一）演练活动期间应确保参加演练部门、人员、物资到位；

（二）演练施行是演练执行的关键阶段，演练各参与方应按照演练方案推动演练过程实施。

（三）演练完毕后发出结束信号并宣布演练结束，对演练场景进行清理和回复，相关参演人员进行总结；

（四）形成演练报告。

第七章　附则

附件 1 联系人名单

职务	姓名	手机号
应急领导小组-组长	毛强华	18501782969
应急领导小组-组员	谷泓睿	18616537791
应急领导小组-组员	李洋	18616361017
应急领导小组-组员	李珂	18721567817
应急领导小组-组员	伍君	18117256257
技术 A 角	林鹏	17301780095
技术 B 角	张佳鹏	15026717338
业务 A 角	管鹏飞	17621892066
业务 B 角	周耀强	15618558749